



**HIRSCHMANN**

A Belden Company

# **User Manual**

## **Basic Configuration**

### **Industrial ETHERNET Gigabit Switch RS20/RS30/RS40, MS20/MS30,**

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2007 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in Germany (9.7.07)

Hirschmann Automation and Control GmbH  
Stuttgarter Straße 45-51  
72654 Neckartenzlingen  
Tel. +49 1805 141538

-01-0607

# Contents

<b>Contents</b>	<b>3</b>
<b>About this Manual</b>	<b>9</b>
<b>Key</b>	<b>11</b>
<b>Introduction</b>	<b>13</b>
<b>1 Access to the user interfaces</b>	<b>15</b>
1.1 System monitor	16
1.2 Command Line Interface	19
1.3 Web based Interface	22
<b>2 Entering the IP parameters</b>	<b>25</b>
2.1 Basics IP parameter	27
2.1.1 IP address (version 4)	27
2.1.2 Network mask	28
2.1.3 Example of how the network mask is used	30
2.2 Entering the IP parameters via CLI	32
2.3 Entering the IP parameters via HiDiscovery	35
2.4 Loading the system configuration from the ACA	37
2.5 System configuration via BOOTP	39
2.6 System configuration via DHCP	43
2.7 System Configuration via DHCP Option 82	46
2.8 System configuration via the Web-based Interface	47
2.9 Faulty Device Replacement	49

<b>3</b>	<b>Loading/saving settings</b>	<b>51</b>
3.1	Loading settings	52
3.1.1	Loading from the local non-volatile memory	53
3.1.2	Loading from the AutoConfiguration Adapter	53
3.1.3	Loading from a file	54
3.1.4	Resetting the configuration to the state on delivery	56
3.2	Saving settings	57
3.2.1	Saving Locally (and on the ACA)	57
3.2.2	Saving into a file on URL	58
3.2.3	Saving into a binary file on the PC	59
3.2.4	Saving as script on the PC	59
<b>4</b>	<b>Loading Software Updates</b>	<b>61</b>
4.1	Loading the Software from the ACA	63
4.1.1	Swapping the software available	63
4.1.2	Starting the software	65
4.1.3	Performing a cold start	65
4.2	Loading the Software from the tftp Server	66
4.3	Loading Software via file selector	68
<b>5</b>	<b>Configuring ports</b>	<b>69</b>
<b>6</b>	<b>Protection from unauthorized access</b>	<b>73</b>
6.1	Password for SNMP access	74
6.1.1	Description Password for SNMP access	74
6.1.2	Entering password for SNMP access	75
6.2	Setting Telnet/Web access	79
6.2.1	Description Telnet/Web access	79
6.2.2	Description Web access	79
6.2.3	Enabling/disabling Telnet/Web access	80
6.3	Disabling HiDiscovery function	81
6.3.1	Description HiDiscovery protocol	81
6.3.2	Disabling HiDiscovery function	82
6.4	Port access control	83
6.4.1	Description port access control	83
6.4.2	Defining port access control	84

<b>7</b>	<b>Synchronizing the System Time of the Network</b>	<b>87</b>
7.1	Entering the Time	88
7.2	SNTP	90
7.2.1	Description SNTP	90
7.2.2	Preparing the SNTP configuration	91
7.2.3	Configuring SNTP	92
7.3	Precision Time Protocol	95
7.3.1	Function description PTP	95
7.3.2	Preparing the PTP configuration	98
7.3.3	Configuring PTP	99
7.4	Interaction PTP and SNTP	102
<b>8</b>	<b>Traffic control</b>	<b>105</b>
8.1	Directed frame forwarding	106
8.1.1	Store-and-forward	106
8.1.2	Multi-address capability	106
8.1.3	Aging of learned addresses	107
8.1.4	Entering static address entries	108
8.1.5	Disabling the specific packet distribution	109
8.2	Multicast application	110
8.2.1	Description multicast application	110
8.2.2	Example of a multicast application	111
8.2.3	Description IGMP snooping	112
8.2.4	Setting multicast applications	112
8.3	Rate Limiter	116
8.3.1	Description Rate Limiter	116
8.3.2	Setting Rate Limiter for RS20/RS30/40, MS20/30, MACH 1000	116
8.4	Prioritization	119
8.4.1	Description Prioritization	119
8.4.2	Tagging	119
8.4.3	Handling of priority classes	121
8.4.4	Setting Prioritization	122
8.5	Flow control	124
8.5.1	Description Flow control	124
8.5.2	Setting flow control	125

8.6	VLANs	126
8.6.1	Description VLANs	126
8.6.2	Configuring VLANs	129
8.6.3	Setting up VLANs	131
8.6.4	Displaying the VLAN configuration	131
8.6.5	Deleting the VLAN settings	132
8.6.6	Example of a simple VLAN	133
<b>9</b>	<b>Operation Diagnostics</b>	<b>141</b>
9.1	Sending traps	142
9.1.1	SNMP trap listing	143
9.1.2	SNMP traps when booting	144
9.1.3	Configuring traps	144
9.2	Monitoring Device Status	147
9.3	Out-of-band signaling	150
9.3.1	Manual setting the signal contact	151
9.3.2	Monitoring correct operation via the signal contact	152
9.3.3	Monitoring the Device Status with a signal contact	153
9.4	Port status indication	154
9.5	Event counter on port level	156
9.6	Displaying the SFP Status	158
9.7	Topology discovery	159
9.7.1	Description Topology discovery	159
9.7.2	Displaying the topology discovery	161
9.8	IP Address Conflict Detection	163
9.8.1	Description of IP address conflicts	163
9.8.2	Configuring ACD	164
9.8.3	Displaying ACD	164
9.9	Reports	166
9.10	Monitoring port traffic (port mirroring)	167
	<b>Appendix A:Setting up the configuration environment</b>	<b>169</b>
A.1	Setting up DHCP/BOOTP Server	170
A.2	Setting up DHCP Server Option 82	176

A.3	tftp server for software updates	181
A.3.1	Setting up the tftp process	182
A.3.2	Software access rights	185
<b>Appendix B:General Information</b>		<b>187</b>
B.1	Hirschmann Competence	188
B.2	FAQ	189
B.3	Management Information BASE MIB	190
B.4	Used abbreviations	193
B.5	List of RFC's	194
B.6	Based IEEE standards	196
B.7	Technical Data	197
B.8	Copyright of integrated software	198
B.8.1	Bouncy Castle Crypto APIs (Java)	198
B.8.2	LVL7 Systems, Inc.	198
B.9	Reader's comments	199
<b>Appendix C:Index</b>		<b>201</b>





# About this Manual

The “Basic Configuration” user manual contains all the information you need to start operating the switch. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The following thematic sequence has proven itself in practice:

- ▶ Set up device access for operation by entering the IP parameters
- ▶ Check the status of the software and update it if necessary
- ▶ Load/Save the configuration
- ▶ Configure the ports
- ▶ Set up protection from unauthorized access
- ▶ Optimize the data transmission with network load control
- ▶ Synchronize system time in the network
- ▶ Function diagnosis

The “Installation” user manual contains a device description, safety instructions, a description of the display, and all the other information that you need to install the device before you begin with the configuration of the device.

The “Redundancy Configuration” user manual contains all the information you need to select a suitable redundancy procedure and configure it.

The “Industrial Protocols” user manual describes how the Switch is connected by means of a communication protocol commonly used in the industry, such as EtherNet/IP or PROFINET.

You will find detailed descriptions of how to operate the individual functions in the “Web-based Interface” and “Command Line Interface” reference manuals.

If you use Network Management Software HiVision you have further opportunities to:

- ▶ have an event logbook.

- ▶ configure the „System Location“ and „System Name“.
- ▶ configure the network address range and SNMP parameters.
- ▶ save the configuration on the Switch.
- ▶ simultaneous configuration of several Switches.
- ▶ configure the relevant ports to be displayed red if there is no link state.

# Key

The designations used in this manual have the following meanings:

► List


□ Work step


■ **Subheading**

[Indicates a cross-reference with a stored link.](#)

**Note:** A note emphasizes an important fact or draws your attention to a dependency.

`Courier font` ASCII representation in user interface

 Execution in the Web-based Interface user interface

 Execution in the Command Line Interface user interface

Symbols used:



Router



Switch



Bridge



Hub



A random computer



Configuration computer



Server

# Introduction

The Switch has been developed for practical application in a harsh industrial environment. Accordingly, the installation process has been kept simple. Thanks to the selected default settings, you only have to enter a few settings before starting to operate the Switch.



# 1 Access to the user interfaces

The Switch has three user interfaces, which you can access via different interfaces:

- ▶ System monitor via the V.24 interface (out-of-band)
- ▶ Command Line Interface (CLI) via the V.24 connection (out-of-band) and Telnet (in-band)
- ▶ Web-based interface via Ethernet (in-band)

# 1.1 System monitor

The system monitor enables you to

- ▶ select the boot operating software,
- ▶ update the operating software,
- ▶ start the selected operating software,
- ▶ end the system monitor,
- ▶ erase the saved configuration and
- ▶ show the bootcode information.

## ■ Opening the system monitor

- ☐ Using a terminal cable (see accessories) connect the
  - V.24 RJ11 socket to
  - either a terminal or a COM port of a PC with terminal emulation according to VT 100(For the physical connection refer to the “Installation user manual“.).

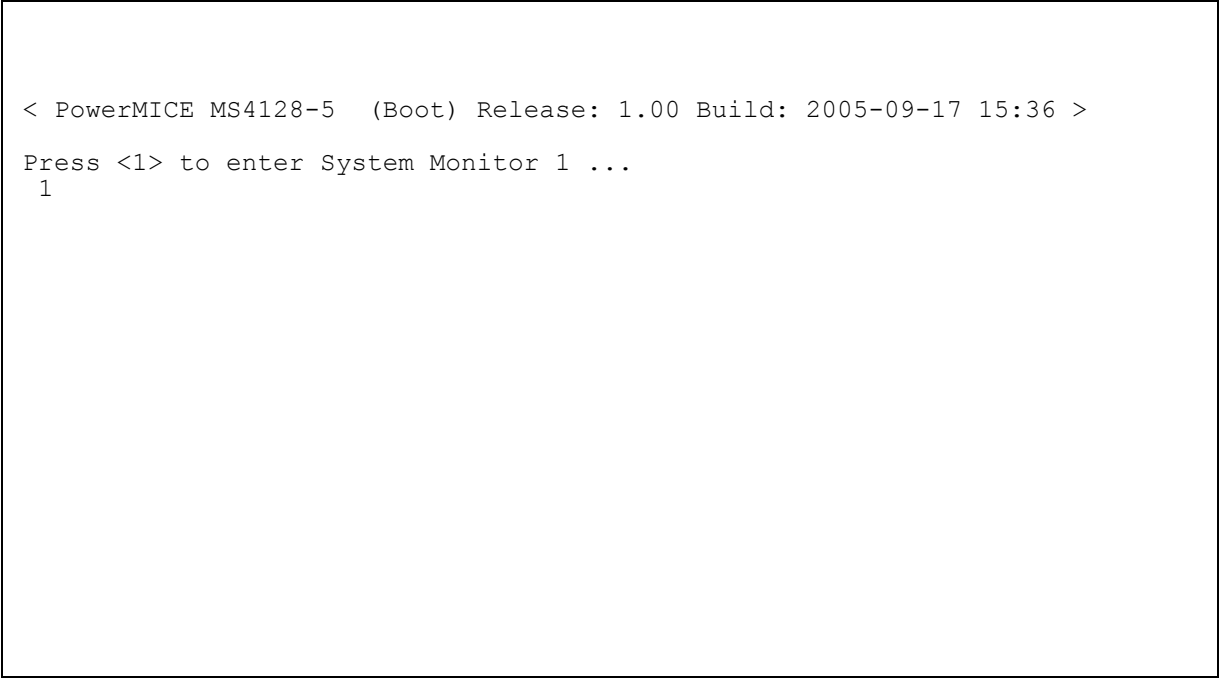
Speed	9.600 Baud
Data	8 bit
Parity	none
Stopbit	1 bit
Handshake	off

*Table 1: Data transfer parameters*

- ☐ Start the terminal program on the PC, and establish a connection with the Switch.

While booting the Switch the message „Press <1> to enter System Monitor 1“ appears on the terminal.





```
< PowerMICE MS4128-5 (Boot) Release: 1.00 Build: 2005-09-17 15:36 >
Press <1> to enter System Monitor 1 ...
1
```

*Fig. 1: Screenshot during the boot process*

- ☐ Press within one second the <1> key to start system monitor 1.

```
System Monitor

(Selected OS: L3P-01.0.00-K16 (2005-10-31 19:32))

1  Select Boot Operating System
2  Update Operating System
3  Start Selected Operating System
4  End (reset and reboot)
5  Erase main configuration file


sysMon1>
```

*Fig. 2: System monitor 1 screen display*

- ☐ Select the desired menu by entering the number.
- ☐ To leave a sub menu and return to the main menu of system monitor 1, press <ESC>.

## 1.2 Command Line Interface

The Command Line Interface allows you to use all device functions via a local or a remote connection.

The command line interface provides IT specialists with a familiar environment for configuring IT devices.

The script ability of the Command Line Interfaces allows to feed several devices with identical configuration data.

For a detailed description of the Command Line Interface, see the Reference Guide „Command Line Interface“.

The Command Line Interface can be accessed via

- ▶ the V.24 (out-of-band) port or
- ▶ Telnet (in-band).

**Note:** To facilitate making entries, the CLI offers the option of abbreviating keywords. Type in the first letters of the keyword. If you now press the Tab key, the CLI will complete the keyword, i.e. add the remaining letters for you.

### ■ Opening the Command Line Interface

- ☐ Connect the Switch via the V.24 interface to a terminal or to a COM port of a PC with terminal emulation according to VT 100 and press any key (see [“Opening the system monitor” on page 16](#)) or start the Command Line Interface via Telnet.  
A window in which you are asked to enter your username appears on the screen.  
A maximum of five users are permitted to access the Command Line Interface.

```
Copyright (c) 2004-2005 Hirschmann Automation and Control GmbH

All rights reserved

PowerMICE Release L3P-01.0.00-K16

(Build date 2005-10-31 19:32)


System Name:  PowerMICE
Mgmt-IP      :  149.218.112.105
1.Router-IP:  0.0.0.0
Base-MAC     :  00:80:63:51:74:00
System Time:  2005-11-01 16:00:59


User:
```

*Fig. 3: Logging in to the Command Line Interface program*

- ☐ Enter a username. The state on delivery value for the username is **admin**. Press the Enter key.
- ☐ Enter the password. The state on delivery value for the password is **private**. Press the Enter key.  
You can change the username and the password later in the Command Line Interface.  
Note that these entries are case-sensitive.

The start screen then appears.

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the 'normal' and 'no' command forms. For the syntax of a particular command form, please consult the documentation.

(Hirschmann PowerMICE) >

*Fig. 4: CLI screen after login*

## 1.3 Web based Interface

The user-friendly Web-based interface gives you the option of operating the Switch from any location in the network via a standard browser such as the Mozilla Firefox or the Microsoft Internet Explorer.

As a universal access tool, the Web browser uses an applet which communicates with the Switch via the Simple Network Management Protocol (SNMP).

The Web-based interface allows you to graphically configure the Switch.

### ■ Opening the Web-based Interface

To open the Web-based interface, you will need a Web browser (a program that can read hypertext), for example Mozilla Firefox version 1 or higher or Microsoft Internet Explorer version 6 or higher.

**Note:** The Web-based interface uses the “Java™ Runtime Environment Version 1.4.2.x, 1.5.x or 6.x” plug-in. If it is not yet installed on your computer, it will be installed automatically via the Internet when you start the Web-based interface. This installation is very time-consuming.

For Windows NT users: cancel the installation. Install the plug-in from the enclosed CD-ROM. Proceed by starting the program file

`jre-6-windows-i586.exe` in the Java directory on the CD-ROM.

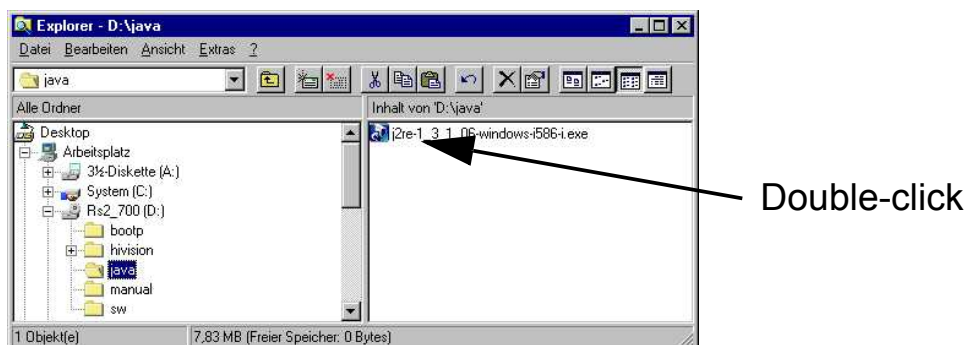
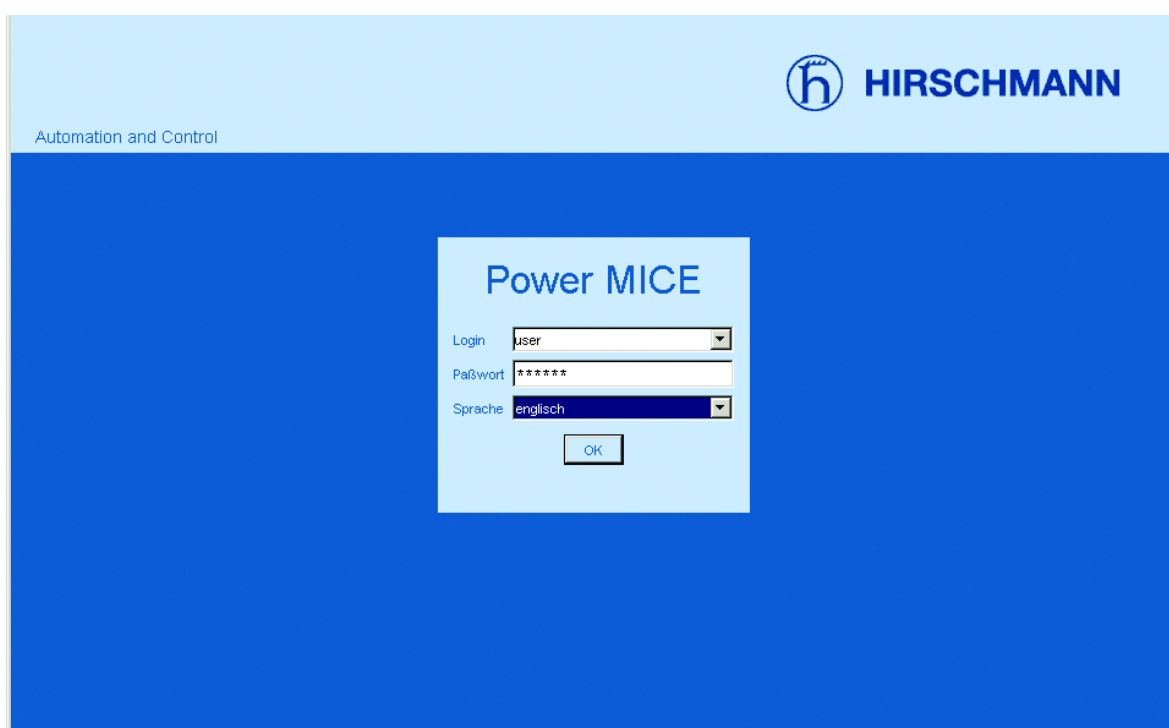


Fig. 5: Install Java

- ☐ Start your Web browser.
- ☐ Make sure that you have activated JavaScript and Java in the security settings of your browser.
- ☐ Establish the connection by entering the IP address of the Switch that you want to administer via the Web-based network management in the address field of the Web browser. Enter the address in the following form:

`http://xxx.xxx.xxx.xxx`

The login window will appear on the screen.



*Fig. 6: Login window*

- ☐ Select the desired language.
- ☐ In the login fold-down menu, select
  - user, for read access or
  - admin, for read and write access to the Switch.

- ☐ The password “public”, with which you have read permission, appears in the password field. If you wish to access the Switch with write permission, then highlight the contents of the password field and overwrite it with the password “private” (state on delivery). Changing the password protects the Switch against unauthorized access.
- ☐ Click on OK.

The Website of the Switch appears on the screen.

**Note:** The changes you make in the dialogs are taken over by the Switch when you click on “Write”. Click on “Load” to update the display.

**Note:** You can block your access to the Switch by entering an incorrect configuration.

Activating the function “Cancel configuration change” in the “Load/Save” dialog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the Switch.



## 2 Entering the IP parameters

IP address(es) must be entered when the Switch is installed for the first time.

The Switch provides 6 options for entering the IP parameters during the first installation:

- ▶ Using the Command Line Interfaces (CLI).  
Choose this “out-of-band” method if
  - you preconfigure your Switch outside its operating environment, or
  - you have no network access (“in-band”) to the Switch(see [“Entering the IP parameters via CLI” on page 32](#)).
- ▶ Using the HiDiscovery protocol.  
Choose this “in-band” method if
  - the Switch is already installed on your network, or
  - if there is another Ethernet connection between your PC and the Switch available.(see [“Entering the IP parameters via HiDiscovery” on page 35](#)).
- ▶ Using the AutoConfiguration Adapter (ACA).  
Choose this method if you are replacing the Switch with a Switch of the same type and have already saved the configuration on an ACA (see [“Loading from the AutoConfiguration Adapter” on page 53](#)).
- ▶ Using BOOTP.  
Choose this “in-band” method if you want to configure the installed Switch using BOOTP. You need a BOOTP server for this. The BOOTP server assigns the configuration data to the Switch using its MAC address (see [“System configuration via BOOTP” on page 39](#)). Because the Switch is delivered with “DHCP mode” as the entry for the configuration data reference, you have to reset this to the BOOTP mode for this method.
- ▶ Using DHCP.  
Choose this “in-band” method if you want to configure the installed Switch using DHCP. You need a DHCP server for this. The DHCP server assigns the configuration data to the Switch using its MAC address or its system name (see [“System configuration via DHCP” on page 43](#)).

- Using DHCP Option 82.  
Choose this “in-band” method if you want to configure the installed Switch using DHCP Option 82. You need a DHCP server with Option 82 for this. The DHCP server assigns the configuration data to the Switch using its physical connection (see [“System Configuration via DHCP Option 82” on page 46](#)).

If the Switch already has an IP address and can be reached via the network, then the Web-based interface provides you with another option for configuring the IP parameters.

## 2.1 Basics IP parameter

### 2.1.1 IP address (version 4)

The IP addresses consist of 4 bytes. These 4 bytes are written in decimal notation, separated by a decimal point.

Since 1992, five classes of IP address have been defined in the RFC 1340.

Class	Network address	Host address	Address range
A	1 Byte	3 Bytes	1.0.0.0 to 126.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 to 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 to 223.255.255.255
D			224.0.0.0 to 239.255.255.255
E			240.0.0.0 to 255.255.255.255

*Table 2: IP address classification*

The network address represents the fixed part of the IP address. The worldwide leading regulatory board for assigning Internet addresses is the IANA (Internet Assigned Numbers Authority). If you need an IP address block, contact your Internet-Service-Provider. Internet Service Providers should contact their local higher-level organization:

- ▶ APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region
- ▶ ARIN (American Registry for Internet Numbers) - Americas and Sub-Saharan Africa
- ▶ LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- ▶ RIPE NCC (Réseaux IP Européens) - Europe and Surrounding Regions

0	Net ID - 7 bits		Host ID - 24 bits		Klasse A	
1	0	Net ID - 14 bits		Host ID - 16 bits	Klasse B	
1	1	0	Net ID - 21 bits		Host ID - 8 bit s	Klasse C
1	1	1	0	Multicast Group ID - 28 bits		Klasse D
1	1	1	1	reserved for future use - 28 b its		Klasse E

Fig. 7: Bit representation of the IP address

All IP addresses belong to class A when their first bit is a zero, i.e. the first decimal number is less than 128.

The IP address belongs to class B if the first bit is a one and the second bit is a zero, i.e. the first decimal number is between 128 and 191.

The IP address belongs to class C if the first two bits are a one, i.e. the first decimal number is higher than 191.

Assigning the host address (host id) is the responsibility of the network operator. He alone is responsible for the uniqueness of the IP addresses he assigns.

## 2.1.2 Network mask

Routers and gateways subdivide large networks into subnetworks. The network mask assigns the IP addresses of the individual devices to a particular subnetwork.

The division into subnetworks with the aid of the network mask is performed in much the same way as the division of the network addresses into classes A to C (net id).

In the part of the host address (host id) representing the mask, the bits are set to one. The remaining bits of the host address in the network mask are set to zero (see the following examples).

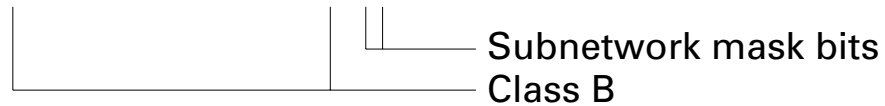
Example of a network mask:

Decimal notation

255.255.192.0

Binary notation

11111111.11111111.11000000.00000000



Example of IP addresses with subnetworks assignment when the above sub-net mask is applied:

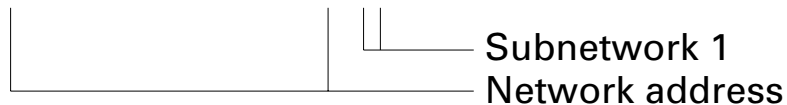
Decimal notation

129.218.65.17



binary notation

10000001.11011010.01000001.00010001



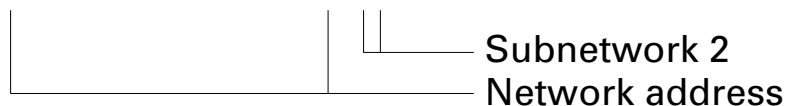
Decimal notation

129.218.129.17



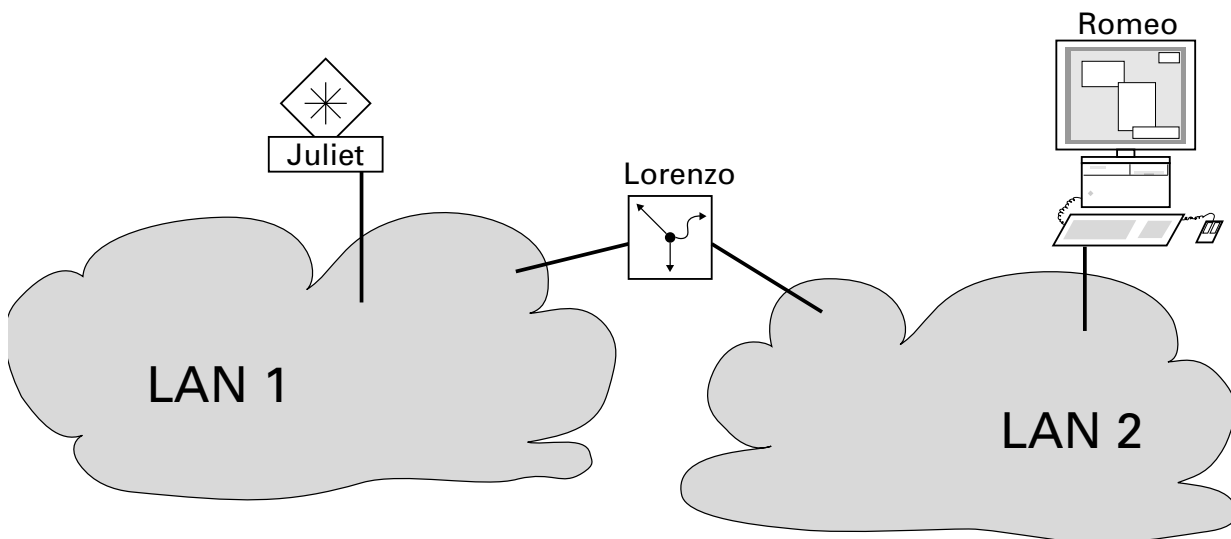
binary notation

10000001.11011010.10000001.00010001



### 2.1.3 Example of how the network mask is used

In a large network it is possible that gateways and routers separate the management agent from its management station. How does addressing work in such a case?



*Fig. 8: Management agent that is separated from its management station by a router*

The management station “Romeo” wants to send data to the management agent “Juliet”. Romeo knows Juliet's IP address and also knows that the router “Lorenzo” knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet's IP address as the destination address. For the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from layer 3 to layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox. This is comparable to going from layer 2 to layer 1, i.e. to sending the data packet over the Ethernet.

Lorenzo receives the letter and removes the outer envelope. From the inner envelope he recognizes that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet's MAC address. He writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo's IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the ISO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo's IP address as destination and her own IP address as source. But where is she to send the answer? For she did not receive Romeo's MAC address. It was lost when Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable `hmNetGatewayIPAddr` as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further envelope with Lorenzo's MAC destination address.

The letter then travels back to Romeo via Lorenzo, the same way the first letter traveled from Romeo to Juliet.

## 2.2 Entering the IP parameters via CLI

If you do not configure the system via BOOTP/DHCP, DHCP Option 82, Hidiscovery protocol or the ACA AutoConfiguration Adapter, then perform the configuration via the V.24 interface using the Command Line Interface:

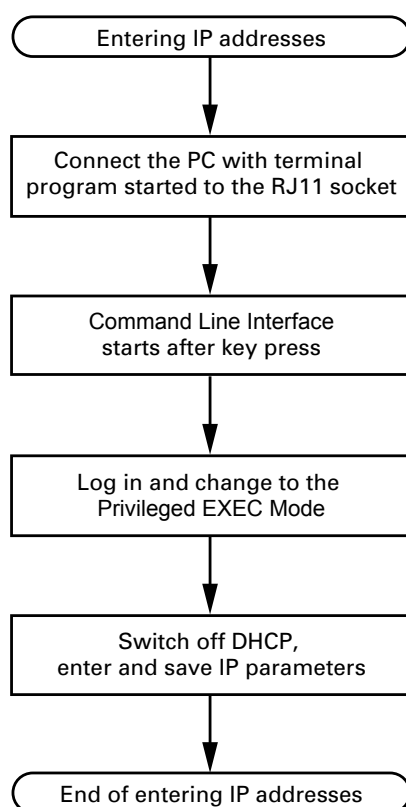


Fig. 9: Flow chart for entering IP addresses

If there is no terminal or PC with terminal emulation available in the vicinity of the installation location, the IP parameters can also be entered in your working environment prior to ultimate installation.

- ☐ Set up a connection with the Switch in accordance with [“Opening the Command Line Interface” on page 19](#).



The start screen then appears

```
NOTE: Enter '?' for Command Help. Command help displays all options  
      that are valid for the 'normal' and 'no' command forms. For  
      the syntax of a particular command form, please consult the  
      documentation.
```

```
(Hirschmann PowerMICE) >
```

- ☐ Change to privileged EXEC mode by entering `enable` and then press the Enter key.
- ☐ Disable DHCP by entering `network protocol none` and then press the Enter key.
- ☐ Enter the IP paremeters with `network parms <IP-Adresse> <Netzmaske> [<Gateway>]` and press the Enter key.
  - ▶ **Locale IP address**  
On delivery, the local IP address of the Switch is 0.0.0.0.
  - ▶ **Network mask**  
If your network has been divided up into subnetworks, and if these are identified with a network mask, then the network mask is to be entered here.  
The default setting of the network mask is 0.0.0.0.

► IP address of the gateway

This entry is only needed if the Switch and the management station/tftp server are located in different subnetworks (see [“Example of how the network mask is used” on page 30](#)).

Enter the IP address of the gateway between the subnetwork with the Switch and the path to the management station.

The default setting of the IP address is 0.0.0.0.

□ Save the configuration entered with

`copy system:running-config nvram:startup-config`  
and then press the Enter key.

Confirm that you want to save the configuration by pressing `y`.

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the 'normal' and 'no' command forms. For the syntax of a particular command form, please consult the documentation.

```
(Hirschmann PowerMICE) >en
(Hirschmann PowerMICE) #network protocol none
(Hirschmann PowerMICE) #network parms 149.218.112.105 255.255.255.0
(Hirschmann PowerMICE) #copy system:running-config nvram:startup-config
Are you sure you want to save? (y/n) y
Copy OK: 15811 bytes copied
Configuration Saved!
(Hirschmann PowerMICE) #
```

After entering the IP parameters, you can easily configure the Switch via the Web-based Interface (see Reference manual „Web-based Interface“).

## 2.3 Entering the IP parameters via HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the Switch via the Ethernet.

You can easily configure additional parameters with the Web-based management (see Reference manual „Web-based Interface“).

Install the HiDiscovery software on your PC. The software is on the CD supplied with the Switch.

- ☐ To install it, you start the installation program on the CD.

**Note:** The installation of HiDiscovery involves installing the WinPcap Version 3.0 software package.

If an earlier version of WinPcap is already installed on the PC, then you must first uninstall it. A newer version remains intact when you install HiDiscovery. However, this can not be guaranteed for all future versions of WinPcap. In the event that the installation of HiDiscovery has overwritten a newer version of WinPcap, then you uninstall WinPcap 3.0 and then re-install the new version.

- ☐ Start the HiDiscovery program.

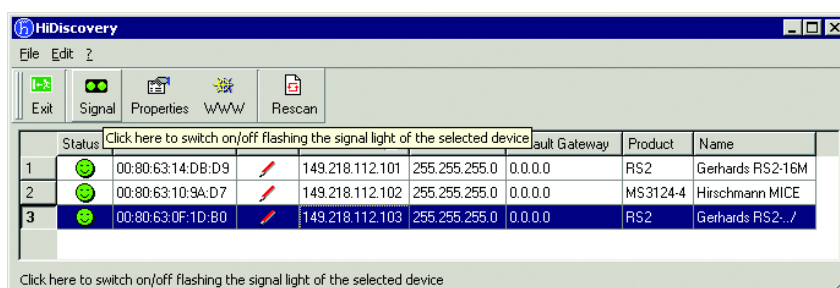


Fig. 10: HiDiscovery

When HiDiscovery is started, it automatically searches the network for those devices which support the HiDiscovery protocol.

HiDiscovery uses the first PC network card found. If your computer has several network cards, you can select these in HiDiscovery on the toolbar.

HiDiscovery displays a line for every device which reacts to the HiDiscovery protocol.

HiDiscovery enables you to identify the devices displayed.

- ☐ Select a device line.
- ☐ Click on the symbol with the two green dots in the tool bar to set the LEDs for the selected device flashing. To Switch off the flashing, click on the symbol again.

By double-clicking a line, you open a window in which you can enter the device name and the IP parameter.

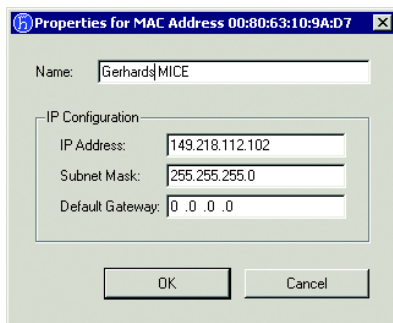


Fig. 11: HiDiscovery - assigning IP parameters

**Note:** After the IP address has been entered, the Switch loads the local configuration settings (see [“Loading/saving settings” on page 51](#)).

**Note:** For security reasons, Switch off the HiDiscovery function for the device in the Web-based interface, after you have assigned the IP parameters to the device (see [“System configuration via the Web-based Interface” on page 47](#)).

**Note:** Save the settings you have made so they will still be available after restart (see [“Loading/saving settings” on page 51](#)).

## 2.4 Loading the system configuration from the ACA

The ACA is a device for

- ▶ storing the configuration data of a Switch.
- ▶ storing the Switch software.

In the case of a Switch failure, the ACA enables a very simple configuration data transfer by means of a substitute Switch of the same type.

When you start the switch, it checks for an ACA. If it detects an ACA with a valid password and valid software, the Switch loads the configuration data from the ACA.

The password is valid if

- ▶ the password on the Switch matches the password on the ACA, or
- ▶ the preset password is entered on the Switch.

To save the configuration data in the ACA see [“Saving Locally \(and on the ACA\)” on page 57](#)

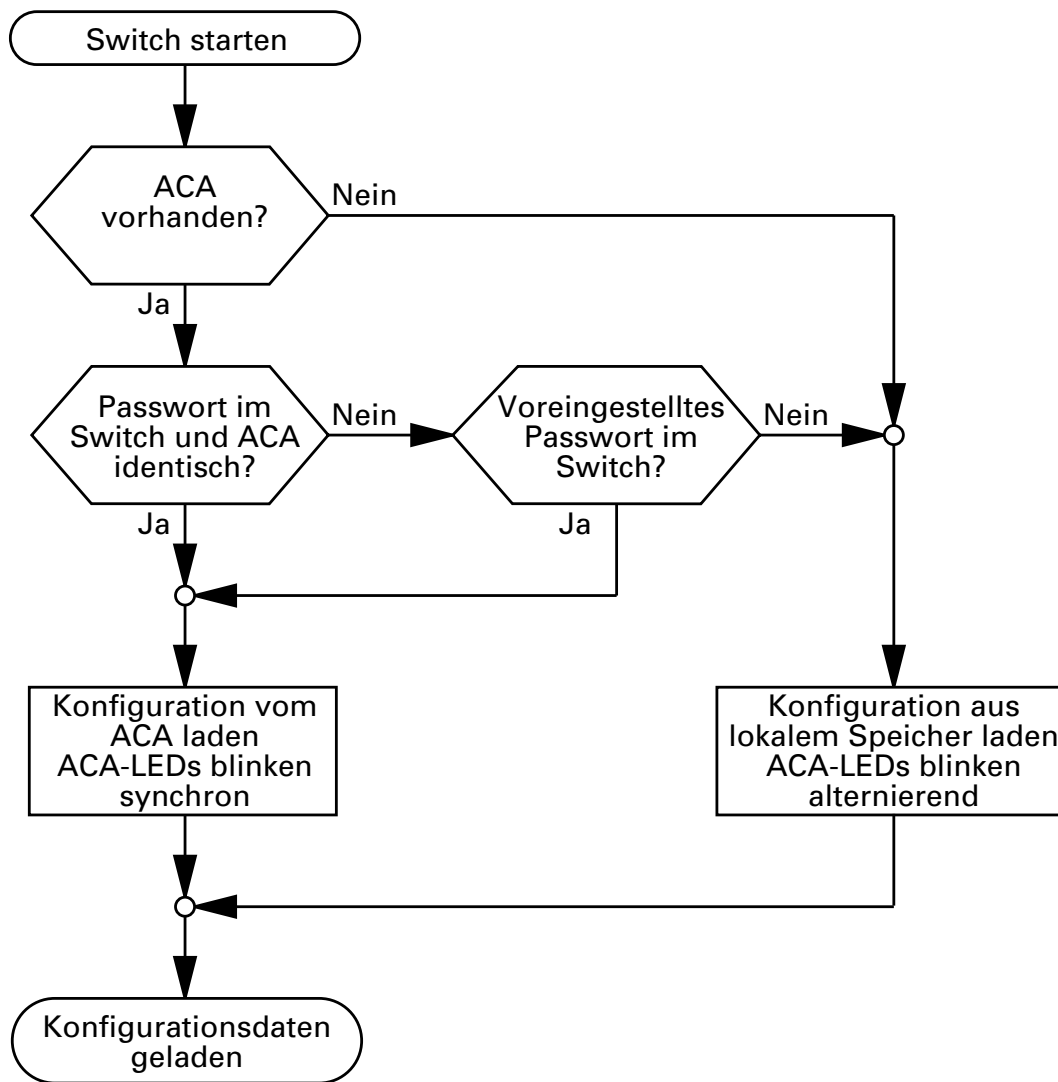


Fig. 12: Flow chart loading configuration data from ACA

## 2.5 System configuration via BOOTP

During startup operation via BOOTP (bootstrap protocol) the Switch receives its configuration data according to the “BOOTP process” flowchart (see Fig. 13).

**Note:** In its state on delivery, the Switch gets its configuration data from the BOOTP server.

- ☐ Activate BOOTP to receive the configuration data, see [“System configuration via the Web-based Interface” on page 47](#) or see in the CLI:

- ☐ Change to the Privileged EXEC mode by entering `enable` and then press the enter key.
- ☐ Enable BOOTP by entering `configure protocol bootp` and then press the enter key.
- ☐ Save the configuration entered with `copy system:running-config nvram:startup-config` and then press the Enter key.  
Confirm that you want to save the configuration by pressing `y`.

- ☐ Make the following data for the Switch available to the BOOTP server:

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateways
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
# tc -- template

.global:\
:gw=0.0.0.0:\
:sm=255.255.240.0:
```

```
switch_01:ht=ether
net:ha=008063086501:ip=149.218.17.83:tc=.global:
switch_02:ht=ether
net:ha=008063086502:ip=149.218.17.84:tc=.global:
.
.
```

Lines that start with a '#' character are comment lines.

The lines under “.global:” make the configuration of several devices easier. With the template (tc) you allocate the global configuration data (tc=.global:). The direct allocation of hardware address and IP address occurs in the device lines (switch-0...).

- ☐ Enter one line for each device.
- ☐ After `ha=` enter the hardware address of the device.
- ☐ After `ip=` enter the IP address of the device.

Refer to [“Setting up DHCP/BOOTP Server” on page 170](#)) for a BOOTP/DHCP server configuration example.



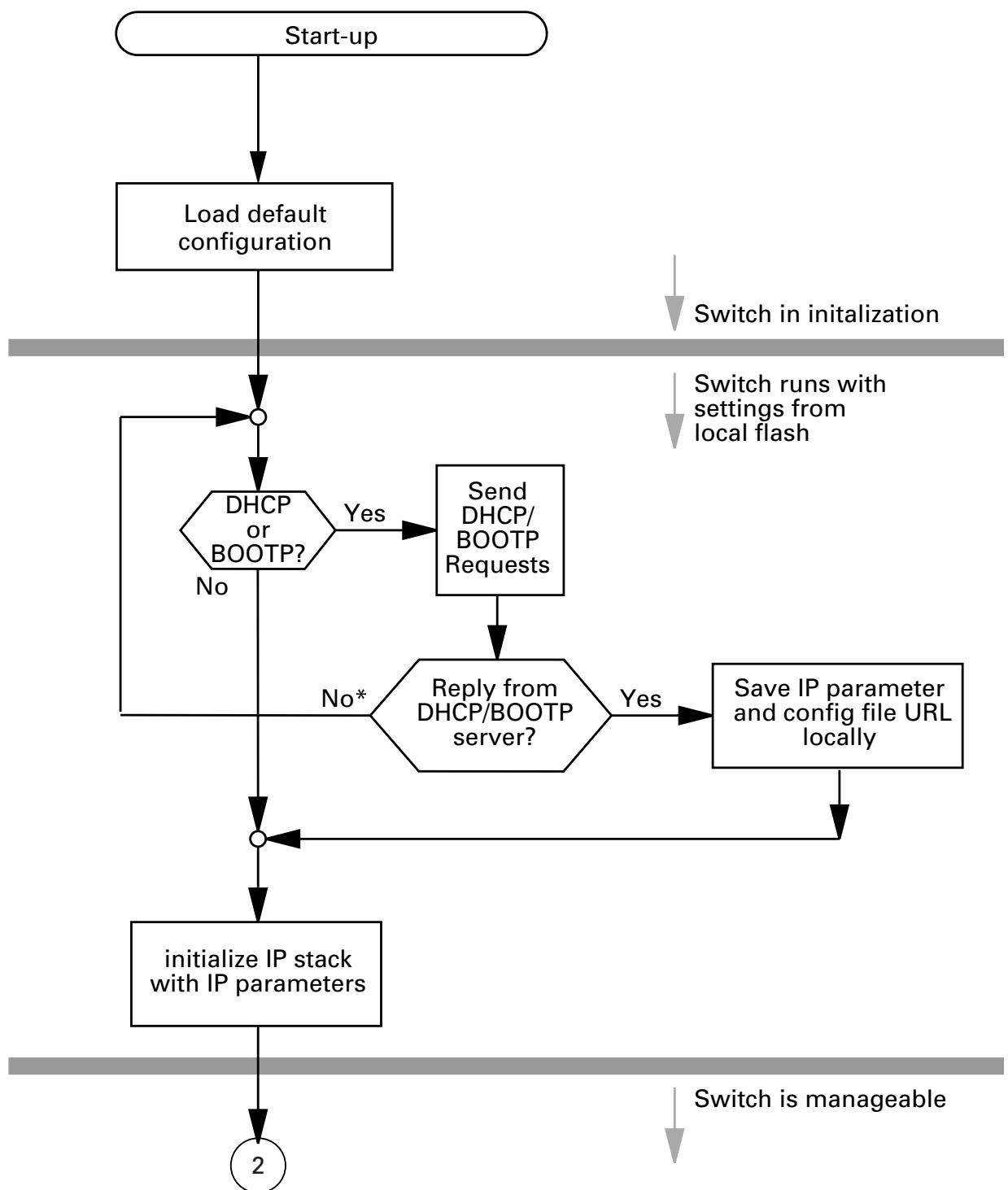


Fig. 13: Flow chart for the BOOTP/DHCP process, part 1  
 \* see note on [page 54](#)

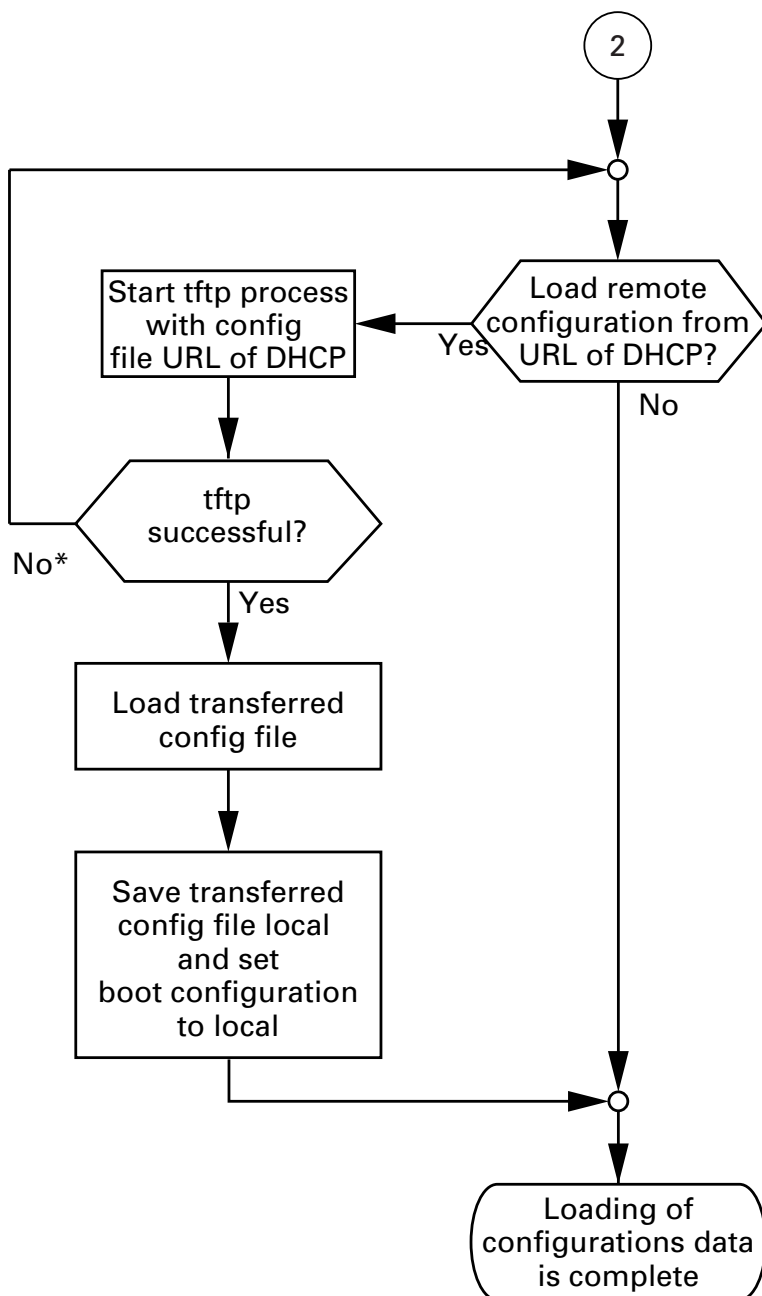


Fig. 14: Flow chart for the BOOTP/DHCP process, part 2  
 \* see note on [page 54](#)

## 2.6 System configuration via DHCP

The DHCP (dynamic host configuration protocol) responds similarly to the BOOTP and offers in addition the configuration of a DHCP client with a name instead of the MAC address. For the DHCP, this name is known as the “client identifier” in accordance with rfc 2131.

The Switch uses the name entered under `sysName` in the system group of the MIB II as the client identifier. You can enter this system name directly via SNMP, the Web-based management (see system dialog), or the Command Line Interface.

On startup, an Switch receives its configuration data according to the “BOOTP/DHCP process” flow chart ([see Fig. 13](#)).

The Switch sends its system name to the DHCP server. The DHCP server can then assign an IP address as an alternative to the MAC address by using the system name.

In addition to the IP address, the DHCP server sends

- the tftp server name (if present),
- the name of the configuration file (if present).

The Switch accepts this data as configuration parameters (see [“System configuration via the Web-based Interface” on page 47](#)).

If an IP address was assigned by a DHCP server, it will be permanently saved locally.

Option	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
61	Client Identifier
66	TFTP Server Name
67	Bootfile name

*Table 3: DHCP options which the Switch requests*

The special feature of DHCP in contrast to BOOTP is that the server can only provide the configuration parameters for a certain period of time (“lease”). When this time period (“lease duration”) expires, the DHCP client must attempt to renew the lease or negotiate a new one. A response similar to BOOTP can be set on the server (i.e. the same IP address is always assigned to a particular client using the MAC address), but this requires the explicit configuration of a DHCP server in the network. If this configuration was not performed, a random IP address – whichever one happens to be available – is assigned.

On delivery DHCP is enabled.

As long as DHCP is activated, the Switch attempts to obtain an IP address. If it cannot find a DHCP server after restarting, it will not have an IP address. To activate/deactivate DHCP, see [“System configuration via the Web-based Interface” on page 47](#).

**Note:** When using HiVision network management, ensure that DHCP always assigns the original IP address to each Switch.

Refer to [“Setting up DHCP/BOOTP Server” on page 170](#)) for a BOOTP/DHCP server configuration example.

Example of a DHCP configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 149.218.112.0 netmask 255.255.240.0 {
    option subnet-mask 255.255.240.0;
    option routers 149.218.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
    hardware ethernet 00:80:63:08:65:42;
    fixed-address 149.218.112,82;
}
```

```
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
# option dhcp-client-identifier "hugo";
  option dhcp-client-identifier 00:68:75:67:6f;
  fixed-address 149.218.112.83;
  server-name "149.218.112.11";
  filename "/agent/config.dat";
}
```

Lines that start with a '#' character are comment lines.

The lines preceding the individually listed devices refer to settings that apply to all the following devices.

The `fixed-address` line assigns a permanent IP address to the device. For further information, please refer to the DHCP server manual.

## 2.7 System Configuration via DHCP Option 82

As with the classic DHCP, on startup an agent receives its configuration data according to the “BOOTP/DHCP process” flow chart (see Fig. 13).

While the system configuration is based on the classic DHCP protocol on the device being configured (see “System configuration via DHCP” on page 43), Option 82 is based on the network topology. This procedure gives you the option of always assigning the same IP address to any device which is connected to a particular location (port of a Switch) on the LAN.

The installation of a DHCP server is described in the chapter “Setting up DHCP Server Option 82” on page 176.

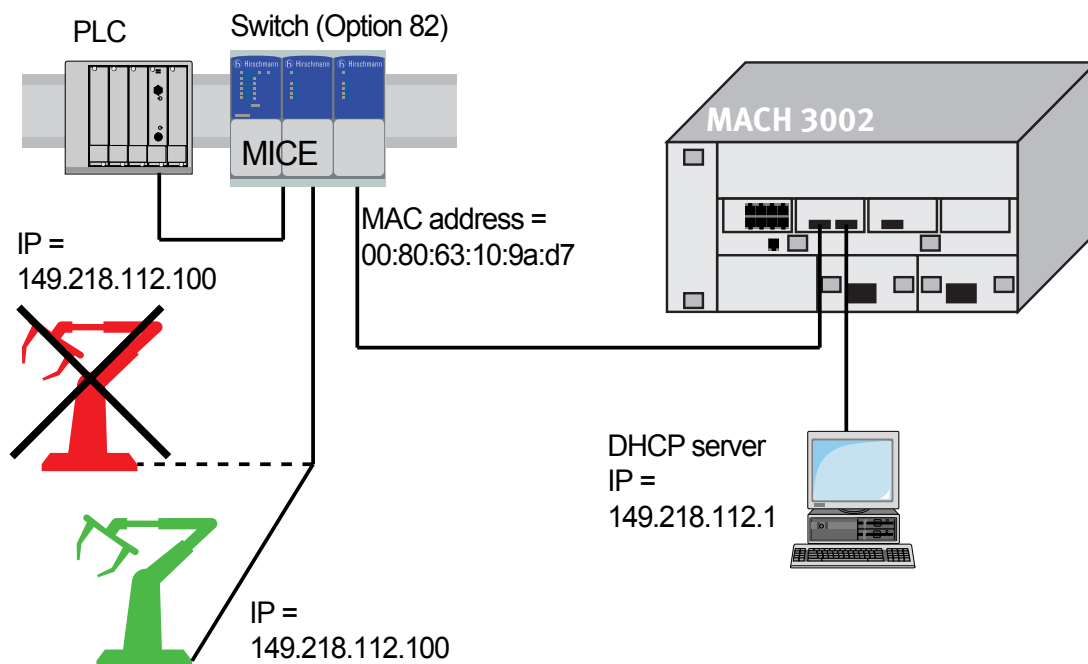


Fig. 15: Application example of using Option 82

## 2.8 System configuration via the Web-based Interface

With the dialog `Basics:Network` you define the source from which the Switch gets its network parameters after starting, assign IP parameters and VLAN ID and configure the HiDiscovery access.

The screenshot shows the 'Network' configuration dialog for a Hirschmann switch. The 'Mode' section has three radio buttons: 'BOOTP', 'DHCP', and 'Local' (which is selected). The 'BOOTP / DHCP' section contains a 'MAC Address' field with the value '00:80:63:51:82:80'. The 'DHCP' section contains a 'System name' field with the value 'PowerMICE\_518280'. The 'Local' section contains three fields: 'IP address' (10.0.1.116), 'Netmask' (255.255.255.0), and 'Gateway address' (0.0.0.0). The 'VLAN' section contains an 'ID' field with the value '1'. The 'HiDiscovery Protocol' section contains an 'Operation' section with 'On' selected and an 'Access' dropdown menu set to 'read-write'. At the bottom of the dialog are three buttons: 'Set', 'Reload', and 'Help'.

Fig. 16: Dialog network parameter

- ☐ Under “Modus” you enter where the Switch is to obtain its IP parameters:
  - ▶ In the BOOTP mode, the configuration comes from a BOOTP or DHCP server on the basis of the MAC address of the Switch (see [page 39](#)).
  - ▶ In the DHCP mode, the configuration comes from a DHCP server on the basis of the MAC address or the name of the Switch (see [page 43](#)).
  - ▶ In the local mode the net parameters in the Switch memory are used.

- ☐ Enter the parameters according to the selected mode on the right.
- ☐ You enter the system name applicable to the DHCP protocol in the `Sy`  
`stem` dialog of the Web-based Interfaces, in the “Name” line.
- ☐ In the “Local” frame assign
  - an IP address,
  - a Netmask and
  - a Gateway Address to the Switch.
- ☐ With the “VLAN ID” frame you can assign a VLAN to the Switch. If you enter the illegal VLAN ID “0” here, the agent can be accessed by all VLANs.
- ☐ The HiDiscovery protocol (see [“Entering the IP parameters via HiDiscovery” on page 35](#)) allows you to assign an IP address to the Switch on the basis of its MAC address. Activate the HiDiscovery protocol if you want to assign an IP address to the Switch from your PC with the HiDiscovery software delivered (setting on delivery: active).

**Note:** Save the settings you have made to ensure they are still available after restart (see [“Loading/saving settings” on page 51](#)).



## 2.9 Faulty Device Replacement

There are two plug-and-play solutions available for replacing a faulty Switch with a Switch of the same type (Faulty Device Replacement):

- ▶ First, you can configure the new switch using an AutoConfiguration Adapter (see [“Loading the system configuration from the ACA” on page 37](#)) or
- ▶ Second, you can configure the new switch using DHCP Option 82 (see [“System Configuration via DHCP Option 82” on page 46](#)).

In both cases, the same configuration data which the faulty Switch had are transferred to the new Switch during booting.



## 3 Loading/saving settings

The Switch saves settings such as the IB parameters and the port configuration in the temporary memory. These settings are lost when you switch off or reboot the device.

The Switch enables you to

- ▶ save settings from the temporary memory in a permanent memory
- ▶ load settings from a permanent memory into the temporary memory.

## 3.1 Loading settings

During restart, the Switch automatically loads its configuration data from the local non-volatile memory, provided that you have not activated BOOTP/ DHCP and that no ACA is connected to the Switch.

During operation, the Switch enables you to load settings from the following sources:

- ▶ the local non-volatile memory,
- ▶ the AutoConfiguration Adapter. If an ACA is connected to the Switch, the Switch always loads its configuration from the ACA.
- ▶ a file in the connected network (= state on delivery)
- ▶ a binary file or an editable and readable script on the PC and
- ▶ the state on delivery.

**Note:** When loading a configuration, do not access the Switch until it has loaded the configuration file and has made the new configuration settings. Depending on the complexity of the configuration settings, this procedure can last between 10-200 seconds.

### 3.1.1 Loading from the local non-volatile memory

When loading the configuration data locally, the Switch loads the configuration data from the local permanent memory if no ACA is connected to the Switch.

- ☐ Select the `Basics:Load/Save` dialog.
- ☐ Click in the “Load”-frame “Local”.
- ☐ Click “Load configuration”.

- ☐ Enter the command `enable` to change to the Privileged EXEC mode.
- ☐ Enter the command  
`copy nvram:startup-config system:running-config`  
to load the configuration data from the local non-volatile memory.

### 3.1.2 Loading from the AutoConfiguration Adapter

If an ACA is connected to the Switch, the Switch always loads its configuration from the ACA.

For information on how to save a configuration file onto an ACA, refer to [“Saving Locally \(and on the ACA\)” on page 57](#).

### 3.1.3 Loading from a file

The Switch allows you to load the configuration data from a file in the connected network if there is no AutoConfiguration Adapter connected to the Switch.

- ☐ Select the `Basics:Load/Save` dialog.
- ☐ Click in the `Load`-frame “fromURL”, if you want the Switch to load the configuration data from a file and to retain the locally saved configuration.  
Click in the `Load`-frame “from URL & save local”, if you want the Switch to load the configuration data from a file and to save this configuration locally.  
“via PC (script/binary)” when you want the Switch to load the configuration data from a file from the PC and retain the locally saved configuration.
- ☐ In the “URL” edit box, type the field path under which the Switch finds the configuration file if you want to load from URL.
- ☐ Click “Load configuration”.

The URL identifies the path to the tftp server from which the Switch loads the configuration file. The URL is in the form  
tftp://IP address of the tftp server/path name/file name  
(e.g. `tftp://149.218.112.5/switch/config.dat`).

Example of loading a file from the TFTPServer

- ☐ To enable yourself to download a file from the tftp server, save the configuration file into the corresponding path of the tftp server with the file name, e.g.. `switch/switch_01.cfg` (see [“Saving into a file on URL” on page 58](#)).
- ☐ Enter the path to the tftp server into the line “URL”, e.g.  
`tftp://149.218.112.214/switch/switch_01.cfg`.

**Note:** The status of the load, started by DHCP/BOOTP (see [“System configuration via BOOTP” on page 39](#)), is displayed in the selected option “from URL & save local” in the “Load” frame. If you get an error message while saving the configuration, one reason may be that loading is not completed. DHCP/BOOTP does not finish loading until a valid configuration is loaded. If DHCP/BOOTP does not find any valid configuration you can stop the active loading by loading the local configuration in the “Load” frame.

Load/Save

HIRSCHMANN

Load

☒ from Switch ☐ from URL ☐ from URL & save to Switch ☐ via PC (script / binary) Load configuration

Save

☒ to Switch ☐ to URL (binary) ☐ to URL (script) ☐ to PC (binary) ☐ to PC (script) Save configuration

URL:

Delete

☒ current configuration ☐ current configuration and from Switch Delete configuration

AutoConfiguration Adapter

Status:

Undo modifications of configuration

Function ☐ Period to undo while connection is lost [s]

Set Reload Help


Fig. 17: Dialog Load/Save

- ☐ Enter the `enable` command to change to the Priviledged EXEC mode.
- ☐ Enter the command  
`copy tftp://149.218.112.159/switch/config.dat nv ram:startup-config` if you want the switch to load the configuration data from a tftp server in the connected network.

### 3.1.4 Resetting the configuration to the state on delivery

The Switch gives you the option to,

- ▶ reset the current configuration to the state on delivery. The locally saved configuration remains.
- ▶ reset the Switch to the state on delivery. After restarting, the IP address is also in the original delivery state.

- 
- ☐ Select the `Basics:Load/Save` dialog.
  - ☐ Make your choice in the “Delete”-frame.
  - ☐ Click “Delete configuration”.

Setting in the System Monitor:

- ☐ Select 5 “Erase main configuration file”  
This menu offers you the possibility to set the Switch to its state of delivery. Configurations being different from the state of delivery are saved in the flash memory in the `switch.cfg` file by the Switch.
- ☐ Press the enter key to erase the `switch.cfg` file.



## 3.2 Saving settings

The Switch enables you to save the settings you have made

- ▶ locally
- ▶ locally and on the ACA, or
- ▶ into a file.

### 3.2.1 Saving Locally (and on the ACA)

The Switch allows you to save the current configuration data in the local permanent memory and the ACA.

- ☐ Select the `Basics:Load/Save` dialog.
- ☐ Click in the “Save”-frame “to Switch”.
- ☐ Click “Save configuration”.

As a result, the Switch saves the current configuration data into the local nonvolatile memory and, provided that an ACA is connected, also into the ACA.

- ☐ Enter the `enable` command to change to the Privileged EXEC mode.
- ☐ Enter the command  
`copy system:running-config nvram:startup-config`  
to save the current configuration data into both the local non-volatile memory and into the ACA if an ACA is connected.

### 3.2.2 Saving into a file on URL

The Switch allows you to save the current configuration data in a file in the connected network.

- ☐ Select the `Basics:Load/Save` dialog.
- ☐ In the “Save” frame, click on “in URL (binary)” to receive a binary file, or “in URL (script)” to receive an editable and readable script.
- ☐ Type in the “URL” edit field the path under which you want the Switch to save the configuration file.
- ☐ Click “Save configuration”.

The URL marks the path to the tftp server on which the Switch saves the configuration file. The URL is written as follows:


tftp://IP address of the tftp server/path name/file name,  
(e.g. `tftp://149.218.112.5/switch/config.dat`).

**Note:** The configuration file contains all configuration data, including the password. Thus, note the access rights on the tftp server..

- ☐ Enter the `enable` command to change to the Privileged EXEC mode.
- ☐ Enter the command  
`copy nvram:startup-config tftp://149.218.112.159/switch/config.dat` if you want the Switch to save the current configuration data into a binary file on a tftp server in the connected network.
- ☐ Enter the command  
`copy nvram:startup-config tftp://149.218.112.159/switch/config.txt` if you want the Switch to save the current configuration data into a script file on a tftp server in the connected network.


### 3.2.3 Saving into a binary file on the PC

The Switch allows you to save the current configuration data in a binary file on your PC.

- 
- ☐ Select the `Basics:Load/Save` dialog.
  - ☐ Click in the "Save"-frame „to PC (binary)".
  - ☐ Enter in the "Save"-window the file name under which you want the Switch to save the configuration file.
  - ☐ Click "Save configuration".

### 3.2.4 Saving as script on the PC

The Switch allows you to save the current configuration data in a editable and readable file on your PC.

- 
- ☐ Select the `Basics:Load/Save` dialog.
  - ☐ Click in the "Save"-frame „to PC (script)".
  - ☐ Enter in the "Save"-window the file name under which you want the Switch to save the configuration file.
  - ☐ Click "Save configuration".



## 4 Loading Software Updates

Hirschmann is continuously working on improving the performance of its products. So it is possible that you may find a more up to date release of the Switch software on the Hirschmann Internet site than the release the you have on your Switch.

### ■ Checking the software release installed

- ☐ Select the `Basics:Software` dialog.  
This dialog views the release number of the software installed on your ACA.

```
enable
show sysinfo
```

Switch to Privileged EXEC mode.  
Display the system information.

```
Alarm..... None

System Description..... Hirschmann Rails
witch
System Name..... RS-1F1054
System Location..... Hirschmann Rails
witch
System Contact..... Hirschmann Automa
tion and Control GmbH
System Up Time..... 0 days 0 hrs 45
mins 57 secs
System Date and Time (local time zone)..... 2007-04-21 08:00:06
System IP Address..... 10.0.1.13
Boot Software Release..... L2E-01.0.00
Boot Software Build Date..... 2005-11-03 13:50
OS Software Release..... L2E-03.1.00
OS Software Build Date..... 2007-06-21 06:14
Hardware Revision..... 1.22 / 4 / 0103
Hardware Description..... RS20-
1600T1T1SDAEHH
Serial Number..... 943434023000001191
Base MAC Address..... 00:80:63:1f:10:54
Number of MAC Addresses..... 32 (0x20)
```

### ■ Loading the software

The Switch gives you three options for loading the software:

- ▶ From the ACA 21-USB (out-of-band)
- ▶ Via tftp from a tftp server (in-band)
- ▶ Via a file selector window from your PC

**Note:** The existing configuration of the Switch is still there after the new software is installed.

## 4.1 Loading the Software from the ACA

Like an usual USB stick, you can also connect the ACA 21-USB to an USB port of your PC and copy the Switch software to the main directory of the ACA 21-USB.

- ☐ Connect the ACA 21-USB, to which you have copied the Switch software, to the USB port of the Switch.
- ☐ Open the system monitor. (see [“Opening the system monitor” on page 16](#)).
- ☐ Select 2, and press the ENTER key to copy the software from the ACA 21-USB into the local memory of the Switch.  
On concluding the update, the System Monitor prompts you to press any key to continue..
- ☐ Select 3 to start the new software on the Switch.

In addition, the system monitor features further options in connection with your Switch software:

- ▶ Swapping the software images available
- ▶ Starting the software,
- ▶ Performing a cold start.

### 4.1.1 Swapping the software available

In this menu item of the system monitor you select one of two possible software releases that you want to load.

The following window appears on the screen:

```
Select Operating System Image

(Available OS: Selected: 1.00 (2004-08-26 07:15), Backup: 1.00 (2004-08-
26 07
:15(Locally selected: 1.00 (2004-08-26 07:15))

1  Swap OS images
2  Copy image to backup
3  Test stored images in Flash mem.
4  Test stored images in USB mem.
5  Apply and store selection
6  Cancel selection

sysMon1>
```

*Fig. 18: Update operating system screen display*

### ■ **Swap OS images**

The memory of the Switch offers space for two images of the software. This offers you e.g. the possibility to load a new version of the software without erasing the existing version.

Select 1 to load the other software with the next reboot.

### ■ **Copy image to backup**

Select 2 to save a copy of the active software.

### ■ **Test stored images in flash memory**

Select 3 to test, if the stored images of the software in flash memory contain valid codes.



**■ Test stored images in USB memory**

Select 4 to test, if the stored images of the software in ACA 21-USB contain valid codes.

**■ Apply and store selection**

Select 5 to apply and store the selection of the software.

**■ Cancel selection**

Select Sie 6 to cancel selection and leave this dialogue without changes.

## **4.1.2 Starting the software**

This menu of the System monitor offers you the possibility to start the selected software.

## **4.1.3 Performing a cold start**

This menu of the system monitor offers you the possibility to reset the hardware of the Switch and to reboot.

## 4.2 Loading the Software from the tftp Server

For a tftp update you need a tftp server on which the software to be loaded is stored (see [“tftp server for software updates” on page 181](#)).

- ☐ Select the `Basics:Software` dialog.

The URL identifies the path to the software stored on the tftp server. The URL is in the format `tftp://IP address of the tftp server/path name/file name` (e.g. `tftp://149.218.112.5/mice/mice.bin`).

- ☐ Enter the path of the Switch software.
- ☐ Click “tftp Update” to load the software from the tftp server to the Switch.

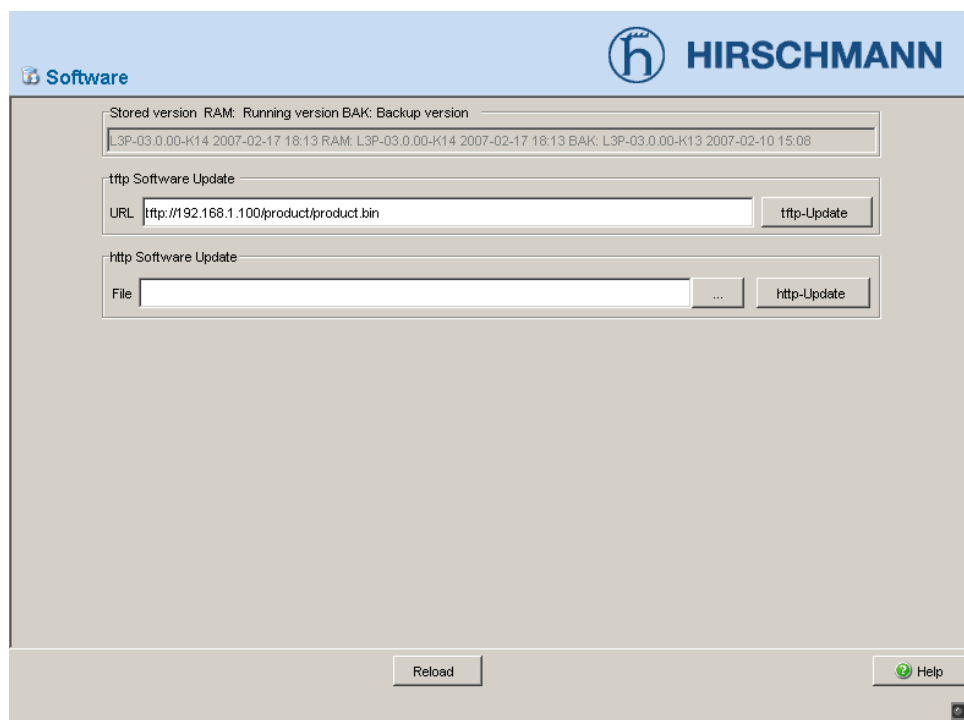


Fig. 19: Software update dialog

- ☐ After the loading procedure has been completed successfully, activate the new software as follows:  
Select the `Basics:Restart` dialog und and perform a cold start.
- ☐ After booting the switch, click “Reload” in your browser to re-enable your access to the Switch.

```
enable
copy tftp://10.0.1.159/
rsL2E.bin system:image
```

Switch to the Privileged EXEC mode.  
Transfer the software file „rsL2E.bin” from the tftp server with the IP address 10.0.1.159 to the Switch.

## 4.3 Loading Software via file selector

For an update via a file selector window you need the Switch software on a drive which you can reach via your PC.

- ☐ Select the `Basics:Software` dialog.
- ☐ In the file selection frame, click on "...".
- ☐ In the file selection window, select the Switch software (switch.bin) and click on "Open".
- ☐ Click "Update", to transfer the software to the Switch.

The end of the update is indicated by one of the following messages:

- ▶ Update completed successfully.
  - ▶ Update failed. Reason: incorrect file.
  - ▶ Update failed. Reason: file damaged.
  - ▶ Update failed. Reason: flash error.
- ☐ After the software procedure has been completed successfully, go to `Basics:Restart`, and perform a cold start ("Restart Switch").
  - ☐ Click "Reload" in your browser to re-enable Switch access after booting.

## 5 Configuring ports

The port configuration consists of:

- ▶ Switching the port on and off,
- ▶ Selecting the operation mode,
- ▶ Displaying connection error messages,
- ▶ Configuring Power over Ethernet.

### ■ Switching the port on and off

In the state on delivery, all ports are switched on. To enhance access security, switch off the ports which you do not wish to connect..

- ☐ Select the `Basics:Port Configuration` dialog..
- ☐ Select in the “Port on” column the ports which are connected to a device.

### ■ Selecting the Operation Mode

In the state on delivery, all ports are switched to the “Automatic Configuration” mode.

- ☐ Select the `Basics:Port Configuration Table` dialog.
- ☐ If the device connected to this port requires a fixed setting
  - select the operation mode (transmission rate, duplex operation) in the “Manual Configuration” colimn, and
  - deactivate the port in the “Autonegotiation” column.

**Note:** The active automatic configuration has priority over the manual configuration.

### ■ **Displaying connection error messages**

In the state on delivery the Switch displays a connection error via the signal contact and the LED display. The Switch allows you to disable the displaying of connection error messages, for instance to prevent a device that has been turned off from being interpreted as an interrupted line.

- ☐ Select the `Basics:Port Configuration` dialog.
- ☐ In the “Signal Contact mask” column, select the ports whose connections you want to have monitored.

### ■ **Configuring Power over ETHERNET**

If the Switch is equipped with PoE media modules, it will then offer you the option of supplying current to devices such as IP phones via the twisted-pair cable. PoE media modules support Power over ETHERNET according to IEEE 802.3af.

The Power over Ethernet function is activated global and on all ports by default.

#### Systempower for MS20/MS30 and Power MICE

The Switch provides the rated system performance for the sum of all PoE ports plus a surplus. Because the PoE media module gets its operating voltage externally, the Switch does not know the possible system power. The Switch therefore assumes a “nominal system power” of 60 Watt per PoE media module for now.

#### System power for MACH 4000

The Switch provides the rated system performance for the sum of all PoE ports plus a surplus. Should the connected devices require more power than is provided by the system, the Switch will then disable the ports. Initially, the Switch disables the ports with the lowest PoE priority. If several ports have the same priority, the switch will first disable the ports with the higher port number.


- ☐ Select the dialog `Basics: Power over Ethernet`.
  - ☐ With “Function On/Off” you turn PoE either on or off.
  - ☐ “Send trap” allows the switch to send a trap in the following cases:
    - Whenever a value exceeds or falls below the performance threshold.
    - When switching the PoE supply voltage on or off on at least one port.
  - ☐ Enter the power threshold in “Threshold”. When this value is exceeded/not achieved, the switch will send a trap, provided that “Send trap” is enabled.

You enter the power threshold as a percentage of the nominal power in relation to the power yielded.
  - ☐ “Nominal Power” displays the performance that the switch nominally provides for all PoE ports together.
  - ☐ “Reserved Power” displays the maximum power that the Switch provides to all the connected PoE devices together on the basis of their classification.
  - ☐ “Delivered Power” indicates how large the current power requirement is at all PoE ports.
- The difference between the “nominal” and “reserved” power indicates how much power is still available to the free PoE ports.

- ☐ In the “Port on” column, you can enable/disable the port.
- ☐ The “Status” column indicates the PoE status of the port.
- ☐ In the “Priority” column (MACH 4000), set the PoE priority of the port to either low, high or critical.
- ☐ The class of the connected device is indicated in the “Class” column:

Class	Maximum power provided
0	15.4 W = State on delivery
1	4.0 W
2	7.0 W
3	15.4 W
4	reserved, treat as class 0
- ☐ The “Name” column indicates the name of the port, see `Basic settings:Port configuration`.

Power over Ethernet

 HIRSCHMANN

Function

☒ On ☐ Off

Send Trap

☒ Yes ☐ No

Threshold [%]

90

Nominal Power [W]

60

Reserved Power [W]

0

Delivered Power [W]

0

Module	Port	Port on	Status	Class	Consumption [W]	Name
4	1	<input checked="" type="checkbox"/>	disabled	-	0.0	
4	2	<input checked="" type="checkbox"/>	disabled	-	0.0	
4	3	<input checked="" type="checkbox"/>	disabled	-	0.0	
4	4	<input checked="" type="checkbox"/>	disabled	-	0.0	

Set

Reload


 Help

Fig. 20: Power over Ethernet dialog



## **6 Protection from unauthorized access**

Protect your network from unauthorized access. The Switch provides you with the following functions for protecting against unauthorized access.

- ▶ Password for SNMP access,
- ▶ Setting the Telnet/Web-Based access,
- ▶ Disabling the HiDiscovery function,
- ▶ Port access control via IP- or MAC-address,

## 6.1 Password for SNMP access

### 6.1.1 Description Password for SNMP access

A network management station communicates with the Switch via the Simple Network Management Protocol.

Every SNMP packet contains the IP address of the sending computer and the password under which the sender of the packet wants to access the Switch MIB.

The Switch receives the SNMP packet and compares the IP address of the sending computer and the password with the entries in the MIB of the Switch (see [“Management Information BASE MIB” on page 190](#)). If the password has the appropriate access right, and if the IP address of the sending computer has been entered, then the Switch will allow access.

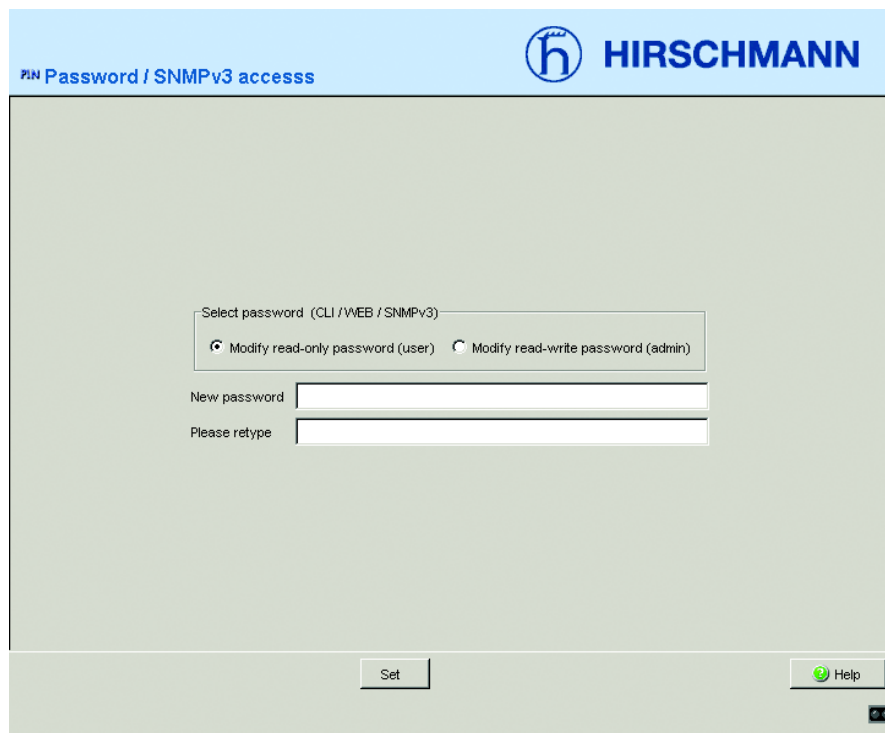
In the delivery state, the Switch is accessible via the “public” password (read only) and the “private” one (read and write) from every computer.

To protect your Switch from unwanted access:

- ☐ First define a new password which you can access from your computer with all rights.
- ☐ Treat this community with discretion. Because everyone who knows the password can access the Switch MIB with the IP address of your computer.
- ☐ Limit the access rights of the known passwords or delete their entries.

## 6.1.2 Entering password for SNMP access

- ☐ Select the `Security:Password / SNMPv3 access` dialog. This dialog gives you the option of changing the read and read/write passwords for access to the Switch via Web-based Interface/CLI/ SNMP. Please note that passwords are case-sensitive. For security reasons, the read password and the read/write password must not be identical.
- ☐ The Web-based Interface and the User Interface communicate via SNMP version 3.
- ☐ Select "Modify read-only password" to enter the read-only password.
- ☐ Enter the new read-only password in the line "New password" and repeat the entry in the line "Please retype".
- ☐ Select "Modify read-write password" to enter the read-write password.
- ☐ Enter the new read-write password in the line "New password" and repeat the entry in the line "Please retype".



The screenshot shows a web-based configuration interface for Hirschmann. At the top, there is a blue header bar with the text "Password / SNMPv3 access" on the left and the Hirschmann logo on the right. The main content area is a light gray rectangle. Inside this area, there is a smaller gray box containing the text "Select password (CLI / WEB / SNMPv3)". Below this text are two radio buttons: "Modify read-only password (user)" which is selected, and "Modify read-write password (admin)". Below the radio buttons are two text input fields: "New password" and "Please retype". At the bottom of the main gray area, there are two buttons: "Set" on the left and "Help" on the right. The "Help" button has a green question mark icon next to it.

Fig. 21: Password dialog

**Important:** If you do not know a password with read/write access, you will not have write access to the Switch!

**Note:** After changing the password for write access, restart the Web interface in order to access the Switch.

**Note:** For security reasons, the passwords are not displayed. Make a note of every change! You cannot access the Switch without a valid password!

**Note:** For security reasons, SNMP version 3 encrypts the password. With the setting SNMPv1 or SNMPv2 in the `Security:SNMPv1/v2 Access` dialog, the password becomes readable again.

**Note:** In SNMP version 3, use 5 up to 32 characters for the password, because many applications do not accept shorter passwords.

- ☐ Select the `Security:SNMPv1/v2 Access` dialog. This dialog gives you the option to select the access via SNMPv1 or SNMPv2. In the state on delivery both protocols are enabled. Thus you can manage the Switch via HiVision and communicate with earlier versions of SNMP.

Please note that passwords are case-sensitive.

Select “SNMPv1/2c on” to be able to communicate with earlier versions of SNMP.

If you select SNMPv1 or SNMPv2 in the table you can determine which IP addresses are allowed to access the Switch and which kind of passwords are to be used.

The table allows up to 8 entries.

For security reasons, the read password and the read/write password must not be identical.

Please note that passwords are case-sensitive.

Index	Current number for this table entry
Password	Password, the computer has to use, to have access to the Switch. This password is independent of the SNMPv3 password.
IP address	IP address of the computer that is allowed to access the Switch.
IP mask	IP mask to the IP address.
Access Mode	Access Mode determines if the computer has read-only or read-write access.
Active	Enabling/Disabling this table entry.

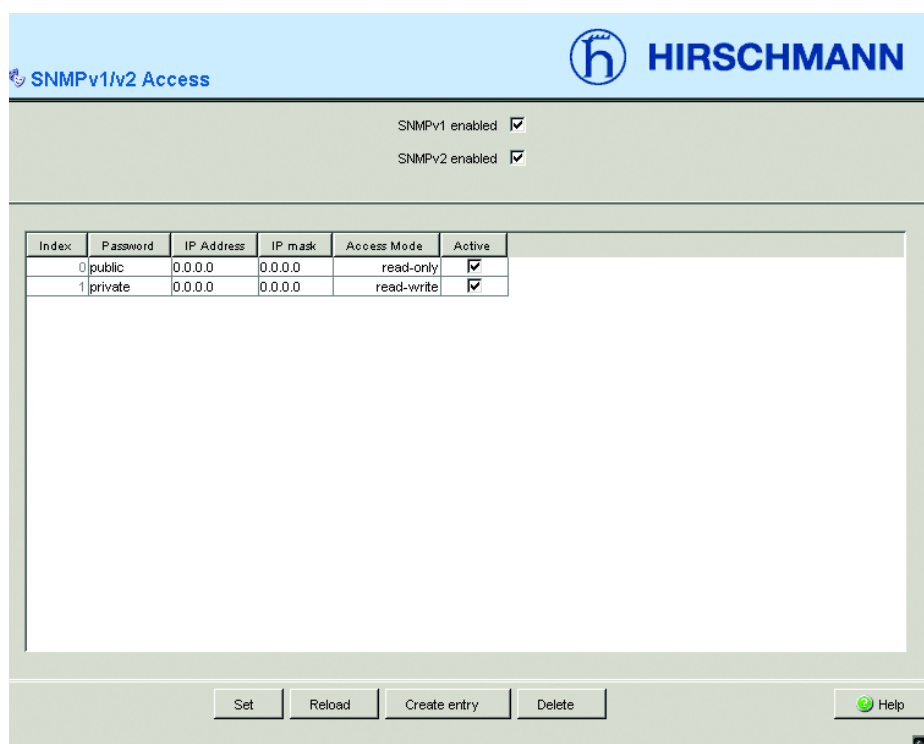


Fig. 22: Dialog SNMPv1/v2 access

- ☐ To create a new line in the table click "Create entry" .
- ☐ To delete an entry select the line in the table and click "Delete".

## 6.2 Setting Telnet/Web access

### 6.2.1 Description Telnet/Web access

The Telnet server of the Switch allows you to configure the Switch using the Command Line Interface (in-band). You can switch off the Telnet server to prevent Telnet access to the Switch.

In the state of delivery, the server is switched on.

After the Telnet server has been switched off, a new access to the Switch with a Telnet connection is not possible. An existing Telnet connection remains.

**Note:** The command line interface (out-of-band) and the `Security:Telnet/Web Access` dialog in the Web-based Interface allow you to activate the telnet server again.

### 6.2.2 Description Web access

The Web server of the Switch allows you to configure the Switch using the Web-based interface. You can switch off the Web server to prevent Web access to the Switch.

In the state of delivery, the server is switched on.

After the Web server has been switched off, a new logon with a Web browser is not possible. The logon in the opened browser window keeps active.

**Note:** The command line interface allows you to activate the Web server again.

### 6.2.3 Enabling/disabling Telnet/Web access

- ☐ Select the `Security:Telnet/Web Access` dialog.
  - ☐ Switch off the server to which you wish to disable access.
- 
- ☐ Enter the command `enable` to switch to the privileged EXEC mode.
  - ☐ Enter the command `transport input telnet` to switch on the telnet server.
  - ☐ Enter the command `no transport input telnet` to switch off the telnet server.
  - ☐ Enter the command `ip http server` to switch on the Web server.
  - ☐ Enter the command `no ip http server` to switch off the Web server.



## 6.3 Disabling HiDiscovery function

### 6.3.1 Description HiDiscovery protocol

The HiDiscovery protocol (see [“Entering the IP parameters via HiDiscovery” on page 35](#)) allows you to assign an IP address to the Switch on the basis of its MAC address. HiDiscovery is a layer 2 protocol.

**Note:** For security reasons, either limit or switch off completely the HiDiscovery function of the Switch after assigning the IP parameters.

## 6.3.2 Disabling HiDiscovery function

- ☐ Select the `Basics:Network.` dialog.
  - ☐ Switch off the HiDiscovery function in the “HiDiscovery Protocol” frame, or limit access to “read-only”.
- 
- ☐ Enter the command `enable` to switch to the privileged EXEC mode.
  - ☐ Enter the command `network protocol hidiscovery off` to switch off the HiDiscovery function.
  - ☐ Enter the command `network protocol hidiscovery read-only` to switch on the HiDiscovery function with the read-only access right.
  - ☐ Enter the command `network protocol hidiscovery read-write` to switch on the HiDiscovery function with the read-write access right.

## 6.4 Port access control

### 6.4.1 Description port access control

The Switch protects every port from unauthorized access.

Depending of your choice the Switch checks the MAC address or the IP address of the connected device.

The following functions are available for monitoring every individual port:

► Who has access to this port?

The Switch recognizes 2 classes of access control:

- All: no access restriction  
MAC address 00:00:00:00:00:00 oder  
IP address 0.0.0.0.
- User: only an assigned user has access.  
the user you define by his MAC address or his  
IP address.

► What should happen after an unauthorized access attempt?

The Switch can respond in three selectable ways to an unauthorized access attempt:

- non: no response
- trapOnly: message by sending a trap
- portDisable: message by sending a trap and  
disabling a port

**Note:** Since the Switch is a layer 2 device, it translates the stored IP addresses into MAC addresses. This requires that a MAC address be assigned to exactly one IP address.

Please keep in mind that when using a router, several IP addresses can be assigned to one MAC address, namely that of the router. This means that all packets of the router will pass the port unchecked if the permitted IP address is that of the router.

If a connected device sends packets with other MAC addresses and a permitted IP address, the Switch will disable the port.

## 6.4.2 Defining port access control

- ☐ Select the `Security:Port Security` dialog.
- ☐ First select, whether you wish the MAC based or the IP based port security.
- ☐ If you have selected MAC based you enter in the “Allowed MAC addresses” column the MAC addresses of the devices with which a data exchange at this port is permitted. You can enter up to 10 MAC addresses each of these separated with a space character. Without entry, reception from all devices is allowed.
- ▶ The “Current MAC address” column shows the MAC address of the device from which data was last received. By pressing the left mouse button, you can copy an entry from the “Current MAC address” column into the “Allowed MAC address” column.
- ☐ If you selected IP based, enter in the column “Allowed IP addresses” the IP addresses of the devices, with which data exchange at this port is allowed. You can enter up to 10 IP addresses each of these separated with a space character. Without entry, reception from all devices is allowed.
- ☐ In the “Action” column you select whether an unauthorized access attempt should be followed by
  - no action (none) or
  - the sending of an alarm (trapOnly) or
  - switching off the port by making a corresponding entry in the port configuration table (see [“Configuring ports” on page 69](#)) and sending an alarm (trap) (portDisable).

**Port Security**

Configuration

☒ MAC-Based Port Security ☐ IP-Based Port Security

Module	Port	Port Status	Allowed MAC Address	Current MAC Address	Allowed IP address	Action
1	1	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	2	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	3	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
1	4	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
2	1	enabled	00:00:00:00:00:00	00:11:25:07:88:37	0.0.0.0	none
2	2	enabled	00:00:00:00:00:00	00:80:63:14:DB:DF	0.0.0.0	none
2	3	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
2	4	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
3	1	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none
3	2	enabled	00:00:00:00:00:00	00:00:00:00:00:00	0.0.0.0	none

Set Reload Help

Fig. 23: Port Security dialog

**Note:** This entry in the port configuration table is part of the configuration (“Loading/saving settings” on page 51) and is saved together with the configuration.

**Note:** An alarm (trap) can only be sent if at least one recipient is entered under “Configuring traps” on page 144 and both the appropriate status and “Port Security” are marked.



## **7 Synchronizing the System Time of the Network**

The real meaning of the term real time depends on the time requirements of the application.

The Switch provides two options with different levels of accuracy for synchronizing the time in your network.

If you only require accuracies in the order of milliseconds, the Simple Network Time Protocol (SNTP) offers a low-cost solution. Accuracy depends on signal running time.

Areas of application of this protocol are:

- log entries,
- time stamping of production data,
- production control, etc.

The Precision Time Protocol (PTP), which is described in the IEEE 1588 standard, achieves accuracies in the order of fractions of microseconds. This superior method is suitable for process control, for example.

Choose the protocol which best meets your requirements. When using both protocols at the same time, bear in mind that they interact.

## 7.1 Entering the Time

If there is no reference clock available, you can enter the system time in the Switch so that you can use it like a reference clock (see [“PTP Global” on page 99](#) and [“Configuring SNTP” on page 92](#)).

- ☐ Select the `Time` dialog.

This dialog offers you the option of making time-related settings independent of the selected time synchronization protocol.

- ▶ The “IEEE 1588 time” displays the time received via PTP.  
The “SNTP time” displays the time with reference to Universal Time Coordinated (UTC).  
The display is the same worldwide. Local time differences are not taken into account.

- ▶ The “System time” uses “IEEE 1588 / SNTPtime”, allowing for the local time difference from “IEEE 1588 / SNTPtime”.  
“System time” = “IEEE 1588 / SNTPtime” + “Local offset”

- ▶ „Time Source“ displays the origin of the following time. The Switch automatically selects the source with the highest precision.

- ☐ With “Set time from PC”, the Switch takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.

“IEEE 1588 / SNTP time” = “System time” - “Local offset”

- ☐ “Local Offset” is for displaying/entering the time difference between the local time and the “IEEE 1588 / SNTPtime”.  
With “Set offset from PC”, the Switch determines the time zone on your PC and then calculates the local time difference.

**Note:** When setting the time in zones with summer and winter times, make an adjustment for the local offset. The Switch can also get the SNTP server IP address and the local offset from a DHCP server.



- ☐ Enter the command `enable` to switch to the privileged EXEC mode.
- ☐ Enter the command `configure` to change to the configuration mode.
- ☐ Enter the command `sntp time <YYYY-MM-DD HH:MM:SS>` to set the Switch system time.
- ☐ Enter the command `sntp client offset <-1000 to 1000>` to enter the time offset between local time and “IEEE1588/SNTP Time”.

## 7.2 SNTP

### 7.2.1 Description SNTP

SNTP has a hierarchical structure. The SNTP Server places the UTC (Universal Time Coordinated) at disposal. The UTC is the time which is referenced to Universal Time Coordinated. The display is the same worldwide. Local time differences are not taken into account.

The SNTP Client obtains the UTC from SNTP Server.

The Switch supports the SNTP Server and SNTP Client functions.

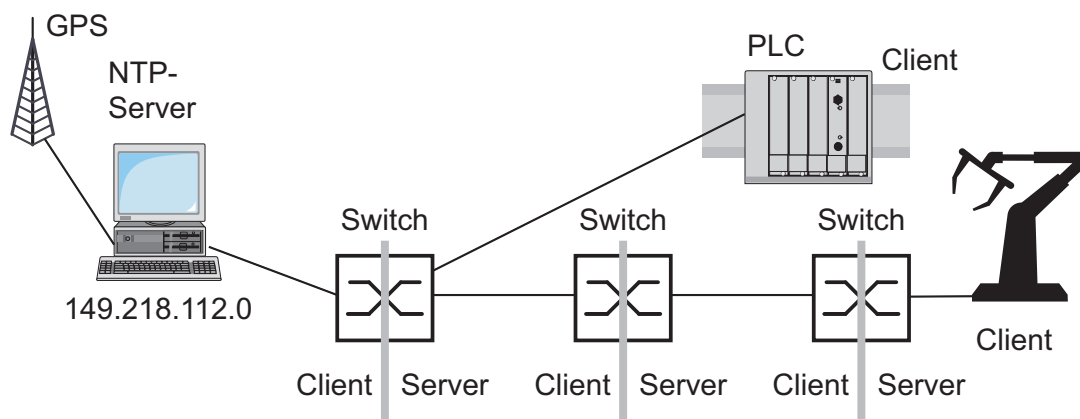


Fig. 24: SNTP cascade

### 7.2.2 Preparing the SNTP configuration

- ☐ To gain an overview of how the system time is passed on, draw a network plan which shows all devices involved in SNTP. Please bear in mind that the accuracy of the system time depends on signal runtime.

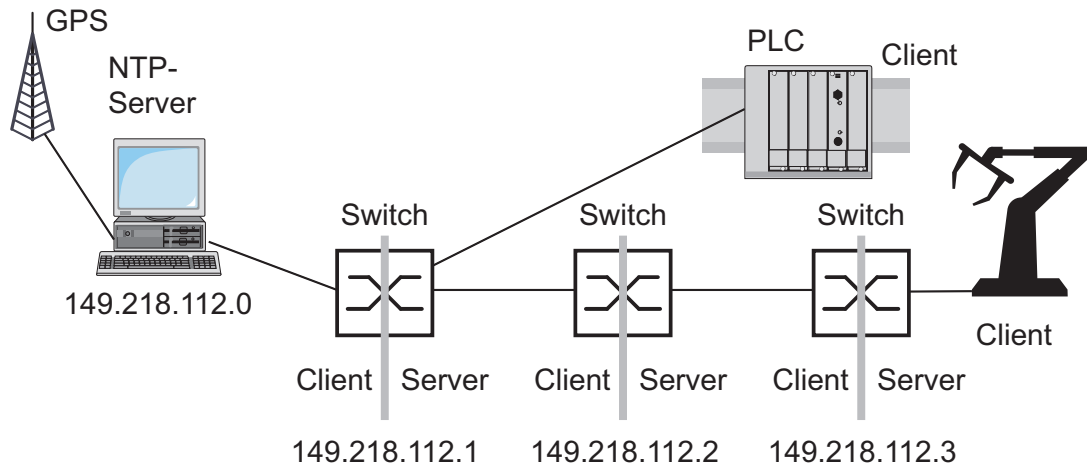


Fig. 25: Example SNTP

- ☐ Switch on the SNTP function on all devices whose time you want to set using SNTP.
- ☐ If you do not have a reference clock at your disposal, use a Switch as the reference clock, and set its system time as accurately as possible.

**Note:** For the most accurate system time distribution possible, avoid having network components (routers, Switches, hubs) which do not support SNTP in the signal path between the SNTP server and the SNTP client.

## 7.2.3 Configuring SNTP

- ☐ Select the `Time : SNTP` dialog.

### ■ Configuration SNTP Client and Server

- ☐ In this frame you Switch the SNTP function on/off.  
When it is switched off,  
the SNTP server does not send any SNTP packages and does not reply to any SNTP requests.  
The SNTP client does not send any SNTP requests and does not interpret any broadcast/multicast packages.

### ■ SNTP-Status

- ▶ The “Status message” displays conditions such as “Server cannot be reached”.

### ■ Configuration SNTP Server

- ☐ In “Anycast destination address” you enter the IP address to which the SNTP server on the Switch sends the SNTP packages.

IP target address	Send SNTP packages periodically to
0.0.0.0	Nobody
Unicast	Unicast
224.0.1.1	Multicast
255.255.255.255	Broadcast

*Table 4: Periodic sending of SNTP packages*

- ☐ In “VLAN ID” you specify the VLAN to which the Switch may periodically send SNTP packages.
- ☐ In “Anycast send interval” you specify the interval at which the Switch sends SNTP packages (valid entries: 1 second to 3600 seconds, default: 120 seconds).

### ■ Configuration SNTP-Client

- ☐ In “External Server Address” you enter the IP address of the SNTP server from which the Switch periodically obtains the system time.
- ☐ In “Redundant Server Address” you enter the IP address of the SNTP server from which the Switch periodically obtains the system time, if the Switch does not receive an answer from the “external server address” 0.5 seconds after making a request.

**Note:** If you are receiving the system time from an external/redundant server address, you do not accept any SNTP broadcasts (see below). Otherwise you can never distinguish whether the Switch is displaying the time from the server entered, or that of an SNTP broadcast package.

- ☐ In “Server request interval” you specify the interval at which the Switch requests SNTP packages (valid entries: 1 second to 3600 seconds, default: 30 seconds).
- ☐ With “Accept SNTP Broadcasts” the Switch takes the system time from SNTP broadcast/multicast packages which it receives.

The screenshot shows the SNTP configuration interface for a Hirschmann switch. The interface is divided into several sections. The top section, 'Configuration SNTP Client And Server', has an 'Operation' toggle set to 'Off'. The 'Configuration SNTP Server' section includes an 'Anycast destination address' dropdown set to '0.0.0.0', an 'Anycast send interval [s]' text box with '120', and a 'Disable Server at local time source' checkbox. The 'SNTP Status' section is currently empty. The 'Configuration SNTP Client' section contains an 'External server address' text box with '0.0.0.0', a 'Redundant server address' text box with '0.0.0.0', a 'Server request interval [s]' text box with '30', a checked 'Accept SNTP Broadcasts' checkbox, a 'Threshold for obtaining the UTC [ms]' text box with '0', and a 'Disable Client after successfull synchronization' checkbox. At the bottom of the dialog are 'Set', 'Reload', and 'Help' buttons.

Fig. 26: SNTP dialog

Switch	149.218.112.1	149.218.112.2	149.218.112.3
Function	on	on	on
Anycast destination address	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN ID	1	1	1
Anycast send interval	120	120	120
Client External server address	149.218.112.0	149.218.112.1	149.218.112.2
Server request interval	30	30	30
Accept SNTP Broadcasts	no	no	no

*Tab. 5: Settings for the example (see Fig. 32)*

## 7.3 Precision Time Protocol

### 7.3.1 Function description PTP

The requirement for running time-critical applications over a LAN is a precise time management system. The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that is based on the principle that one clock is the most precise and makes it possible to synchronize all clocks within a LAN.

This procedure permits synchronization of the clocks with a level of accuracy in the hundreds of nanoseconds. The synchronization messages have virtually no effect on the network load. PTP uses multicast communication.

Factors influencing precision are:

- Accuracy of the reference clock  
IEEE 1588 classifies clocks according to their accuracy. An algorithm that measures the accuracy of the available clocks in the network determines the most accurate time for the “grandmaster” clock.

Stratum number	Specification
0	For temporary, special purposes to assign one clock a better value than all other clocks within the network.
1	Designates the clock with the highest precision as the reference clock. A stratum 1 clock can be both a boundary and an ordinary clock. Stratum 1 clocks include GPS clocks and calibrated atomic clocks. A stratum 1 clock cannot be synchronized via PTP from another clock in the PTP system.
2	Designates the clock as the second-choice reference clock and cannot be synchronized via PTP from another clock in the PTP system.
3	Designates the clock that can synchronize other devices via an external cable as the reference clock.
4	Designates the clock as the reference clock.
5–254	Reserved.
255	Default setting. Such a clock should never be the best master clock.

*Table 6: Stratum – Classifying the clocks*

- Cable delays; device delays  
The communication protocol defined by IEEE 1588 makes it possible to measure cable delays. Formulas for calculating the current time eliminate delays.
- Accuracy of local clocks  
The communication protocol defined by IEEE 1588 takes into account the inaccuracy of local clocks in relationship to the reference clock. Calculation formulas permit the synchronization of the local time, taking the inaccuracy of the local clock into consideration in relationship to the reference clock.

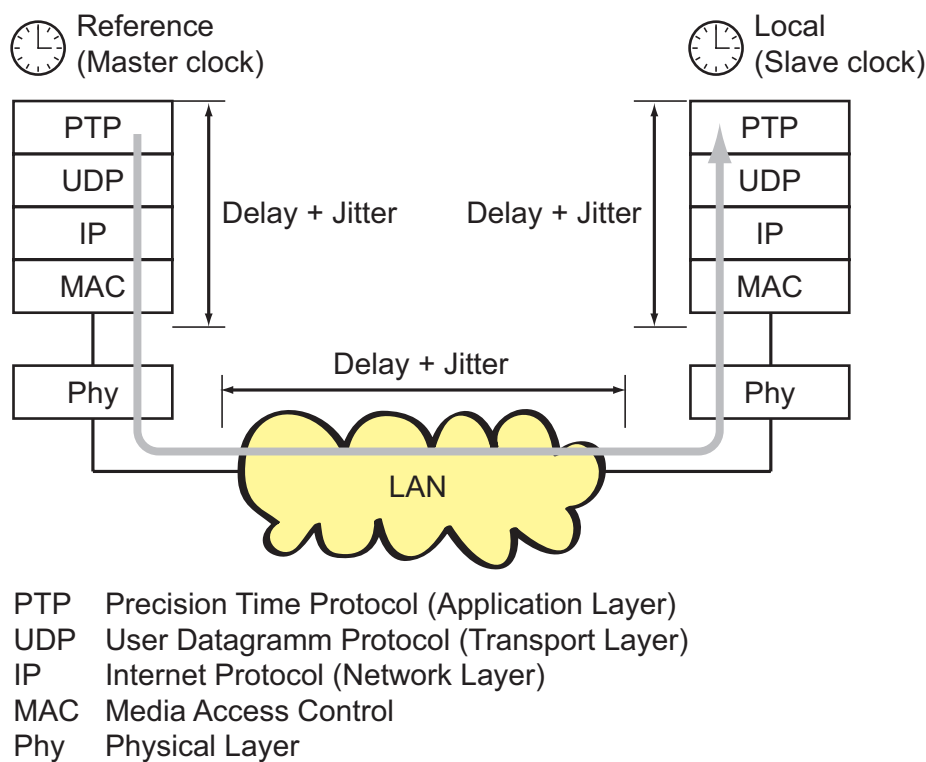


Fig. 27: Delay and jitter problems when synchronizing clocks

To get around the delay and jitter in the protocol stack, IEEE 1588 recommends inserting a special hardware time stamp unit between the MAC and the PHY layer. Devices or modules with the name supplement “RT” are equipped with this time stamp unit.

The delay and jitter in the LAN increase in the media and transmission devices along the transmission path.



The cable delays are relatively constant. Changes occur very slowly. This fact is taken into account by IEEE 1588 by performing measurements and calculations on a regular basis.

IEEE ignores the inaccuracy caused by device delays and device jitter through the definition of “boundary clocks”. Boundary clocks are clocks that are integrated into the devices. These clocks are synchronized on the one side of the signal path and, on the other side of the signal path, are used to synchronize the subsequent clocks (ordinary clocks).

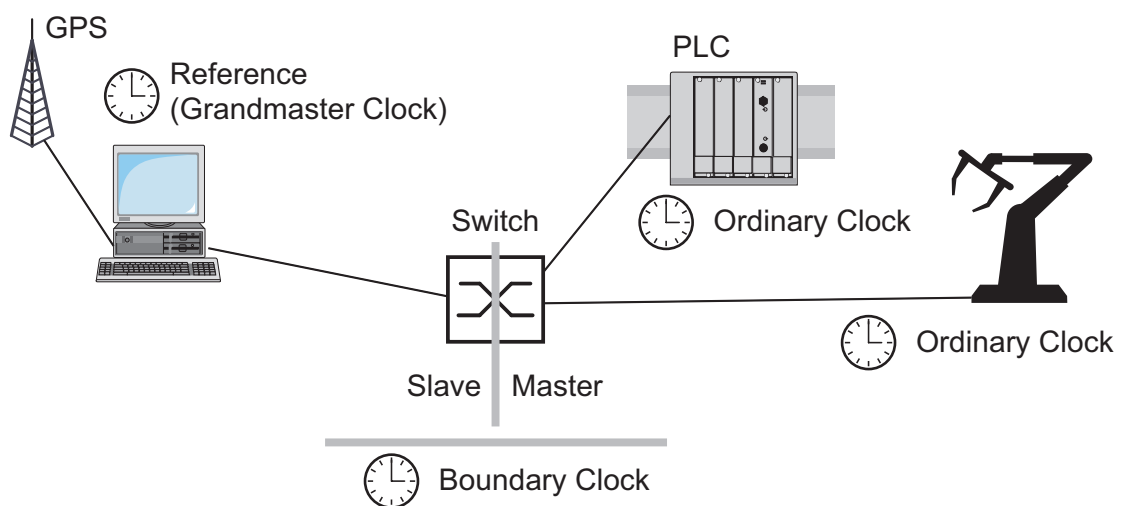


Fig. 28: Boundary Clock

Independent of the physical communication paths, the PTP provides logical communication paths that you define when you set up PTP subdomains. Subdomains are designed to create groups of clocks that are time-independent of the rest of the domain. Typically, the clocks use the same communication paths that other clocks do.

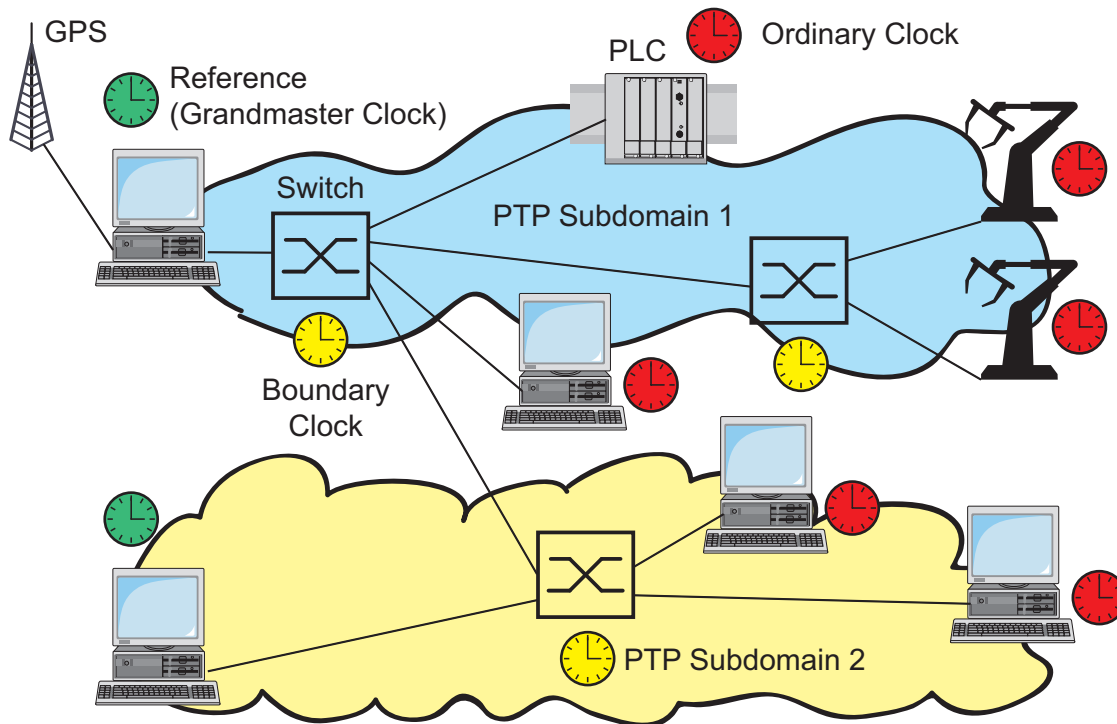


Fig. 29: PTP- subdomains

### 7.3.2 Preparing the PTP configuration

After the function is activated, the PTP takes over the configuration automatically. The original settings in the Switch when it is delivered are sufficient for most applications.

- ☐ Draw a network plan showing all devices involved in PTP to get an overview of the distribution of the clocks.

**Note:** Connect all connections you need to distribute PTP information to devices equipped with an integrated time stamp unit (RT modules). Devices which are not equipped with a time stamp unit obtain the PTP information and set their clocks accordingly. They are not involved in the protocol.

- ☐ Switch on the PTP function on all devices whose time you want to synchronize using PTP.
- ☐ If there is no reference clock available, designate a Switch as reference clock, and set the system time as precisely as possible.

### 7.3.3 Configuring PTP

In the dialog `Time:PTP:Global`, you can enable/disable the function and make the PTP settings on the devices MS20/30 and Power MICE which are to apply to all ports.

#### ■ PTP Global

- ☐ Select the `Time:PTP:Global` dialog.
- ☐ Switch on the function in the “Operation IEEE 1588 / PTP” frame.
- ☐ If you have designated this Switch to be the PTP reference clock, click in the “Configuration IEEE 1588 / PTP” frame in the “Preferred Master” line the value “true”.

► By selecting “Reinitialize” you restart the synchronization of the local clock.

#### ► Configuration

`Clock Mode`: Mode of the local clock.

Possible options are:

- `ptp-mode-Boundary-clock`,
- `ptp-mode-simple-ptp` (without runtime correction, without determining the best clock) Select this mode, if the Switch has no time stamp unit (RT module).

`Preferred Master`: Defines the local clock as the Preferred Master.

**PTP Global** HIRSCHMANN

Operation IEEE 1588 / PTP

Operation ☐ On ☒ Off

Configuration IEEE 1588 / PTP

Clock Mode:

Sync Interval:

Sync Lower Bound [nsec]:

Sync Upper Bound [nsec]:

Subdomain Name:

Preferred Master:

Status IEEE 1588 / PTP

Is Synchronized:

Offset To Master [nsec]:

Max Offset Absolut [nsec]:

Delay To Master [nsec]:

Grandmaster UUID:

Parent UUID:

Clock Stratum:

Clock Identifier:

Set Reload Reinitialize Help

Fig. 30: PTP Global dialog

### Application example:

PTP is used to synchronize the time in the network. As an SNTP client, the left Switch gets the time from the NTP server via SNTP. The Switch assigns clock stratum "2" to the time received from an NTP server. Thus the left Switch becomes the reference clock for the PTP synchronization and is the "preferred master". The "preferred master" forwards the exact time signal via its connections to the RT module. The Switch with RT module receives the exact time signal at a connection of its RT module and thus has the clock mode "ptp-mode-boundary-clock". The Switches without an RT module have the clock mode "ptp-mode-simple-ptp".

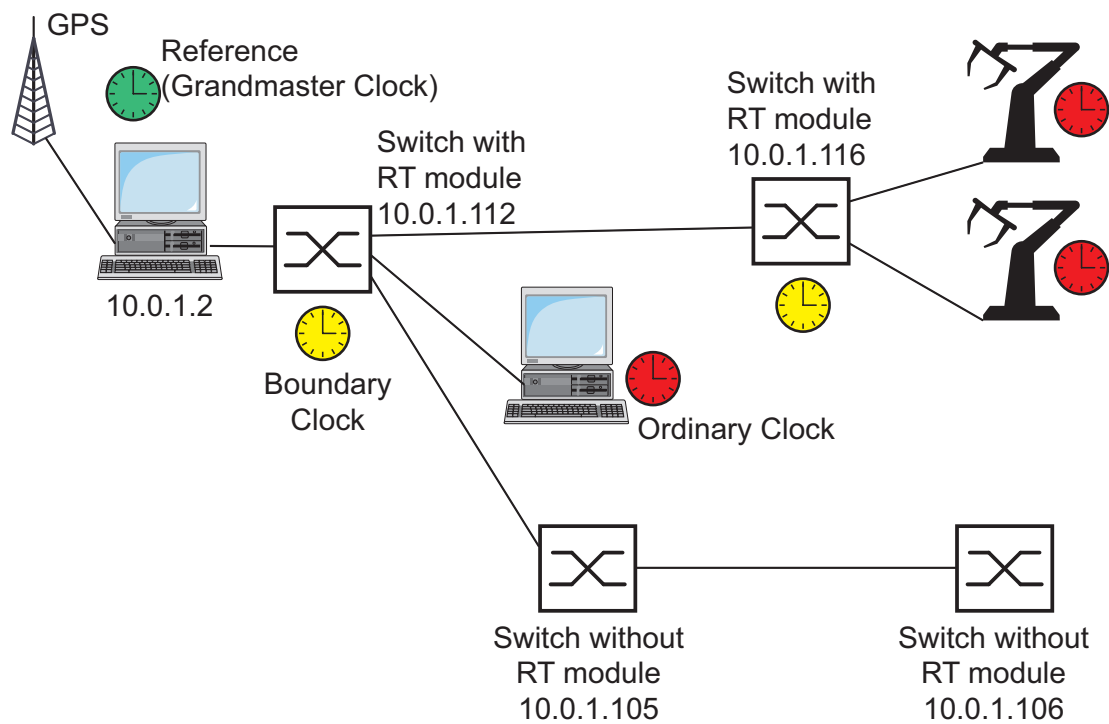


Fig. 31: Example of PTP synchronization

Switch	10.0.1.112	10.0.1.116	10.0.1.105	10.0.1.106
PTP				
Operation	On	On		On
Clock Modus	ptp-mode-boundary-clock	ptp-mode-boundary-clock	ptp-mode-simple-ptp	ptp-mode-simple-ptp
Preferred Master	true	false	false	false
SNTP				
Operation	On	Off	Off	Off
Server destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN ID	1	1	1	1
Client External Server address	10.0.1.2	0.0.0.0	0.0.0.0	0.0.0.0
Request interval	30	arbitrarily	arbitrarily	arbitrarily
Accept SNTP Broadcasts	no	arbitrarily	arbitrarily	arbitrarily

Table 7: Settings for the example (see Fig. 31)

## 7.4 Interaction PTP and SNTP

According to PTP and SNTP, both protocols are permitted to coexist in one network. However, since both protocols influence the system time of the device, situations may occur in which both protocols compete with each other.

**Note:** Configure the devices in such a way that each device receives the system time exclusively from one source.

If you want the switch to receive the system time using PTP, enter the external server address 0.0.0.0, and do not accept any SNTP broadcasts when performing the SNTP client configuration.

If you want the switch to receive the system time using SNTP, make sure that the best clock is connected to the SNTP server. Thus, both protocols receive the time from the same server. The example (see Fig. 32) shows such an application.

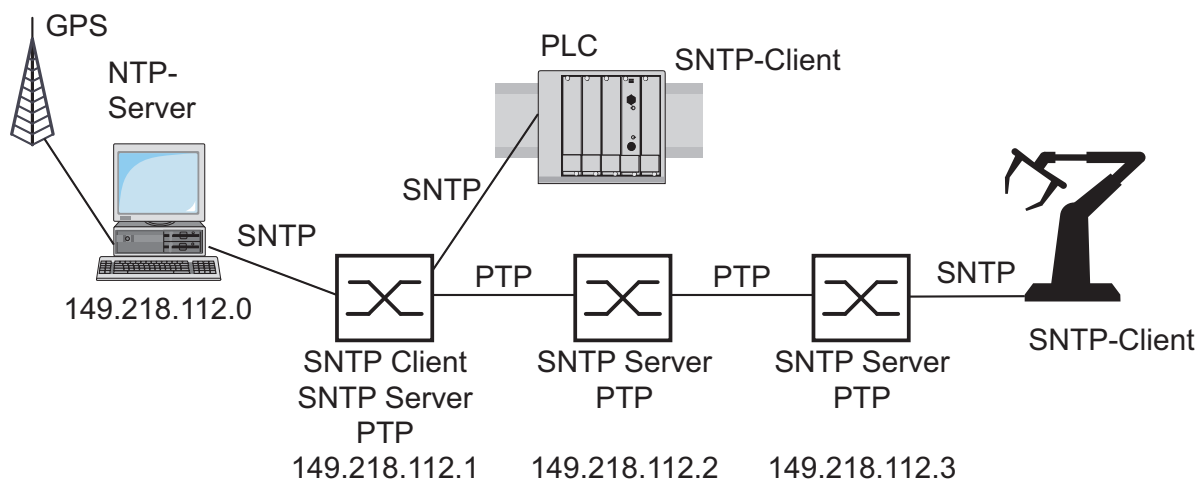


Fig. 32: Example of the coexistence of PTP and SNTP.

### ■ Application example:

The requirements made to network time accuracy are rather high, however the terminal devices exclusively support SNTP (see Fig. 32).

Switch	149.218.112.1	149.218.112.2	149.218.112.3
PTP			
Operation	On	On	On
Clock Mode	ptp-mode-boundary-clock	ptp-mode-boundary-clock	ptp-mode-boundary-clock
Preferred Master	false	false	false
SNTP			
Function	On	On	On
Anycast destination address	224.0.1.1	224.0.1.1	224.0.1.1
Server VLAN ID	1	1	1
Anycast send interval	30	30	30
Client External Server Address	149.218.112.0	0.0.0.0	0.0.0.0
Server request interval	any	any	any
Accept SNTP Broadcasts	no	no	no

*Tab. 8: Settings for the Example*

In the example above, the left switch receives as the SNTP client the system time from the NTP server using SNTP. The switch assigns to a time received from an NTP server the stratum clock number “2”. Thus, the left switch becomes the reference clock for PTP synchronization. PTP is active in all three switches, ensuring that, relative to each other, the system times of the switches are synchronized precisely. As the connectable terminal devices in the example exclusively support SNTP, all three switches serve as SNTP servers.





## 8 Traffic control

To optimize the data transmission, the Switch provides you with the following functions for controlling the network load:

- ▶ Settings for directed frame forwarding (MAC address filter)
- ▶ Multicast settings
- ▶ Rate Limiter
- ▶ Prioritization
- ▶ Flow control
- ▶ Virtual LANs

## 8.1 Directed frame forwarding

Directed frame forwarding is a method used by the Switch to avoid unnecessary increases in the network load. The Switch features the following directed frame forwarding functions:

- ▶ Store-and-forward
- ▶ Multiaddress capability
- ▶ Aging of learned addresses
- ▶ Static address entries
- ▶ Disabling the specific packet distribution

### 8.1.1 Store-and-forward

All data received by the Switch is stored, and its validity is checked. Invalid and defective data packets (> 1,522 Bytes or CRC errors) as well as fragments (< 64 Bytes) are discarded. Valid data packets are forwarded by the Switch.

### 8.1.2 Multi-address capability

The Switch learns all the source addresses for a port. Only packets with

- ▶ unknown addresses
- ▶ these addresses or
- ▶ a multi/broadcast address

in the destination address field are sent to this port. The Switch enters learned source addresses in its filter table (see [“Entering static address entries” on page 108](#)).

The Switch can learn up to 8000 addresses. This becomes necessary if more than one terminal device is connected to one or more ports. It is thus possible to connect several independent subnetworks to the Switch.

### 8.1.3 Aging of learned addresses

The Switch monitors the age of the learned addresses. Address entries which exceed a certain age (30 seconds, aging time) are deleted by the Switch from its address table.

The Switch floods data packets with an unknown target address.

The Switch transmits data packets with known target addresses to specific destinations.

**Note:** A reboot deletes the learned address entries.

- ☐ Select the `Switching:Global` dialog.
- ☐ Enter the Aging Time for all dynamic entries in the range from 10 to 630 seconds (Unit: 1 second, default setting: 30).  
In connection with the router redundancy (see MACH 3000), set the time greater/equal than 30 seconds.

### 8.1.4 Entering static address entries

One of the most important functions of a Switch is the filter function. It selects data packets according to certain defined patterns called filters. These patterns are associated with switching rules. This means that a data packet received at the port of a Switch is compared to the patterns. If there is a pattern which matches the data packet, the Switch will either transmit or reject the packet according to the switching rules for the affected ports.

The following are valid filter criteria:

- ▶ Destination address,
- ▶ Broadcast address,
- ▶ Multicast address,
- ▶ VLAN membership.

The individual filters are stored in the filter table (Forwarding Database, FDB). The table has three parts, a static part and two dynamic parts.

- ▶ The management administrator describes the static part of the filter table (`dot1qStaticTable`).
- ▶ During operation, the Switch is capable of learning which ports will receive data packets from which source addresses (see [“Multi-address capability” on page 106](#)). This information is stored in the dynamic part of the table (`dot1qTpFdbTable`).
- ▶ Addresses learned from the neighbouring agent and those learned by GMRP are written to another dynamic part.

Addresses already located in the static filter table, are automatically transferred by a Switch into the dynamic part.

An address entered statically cannot be overwritten through learning.

**Note:** If the redundancy manager is active, it is not possible to make permanent unicast entries.

**Note:** In the filtering database you can create up to 100 filter for multicast addresses.

- ☐ Select the `Switching:Filter` for MAC addresses dialog.

In the filtering table each row represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the Switch (learned status) or manually. Data packets whose destination addresses are entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination addresses are not in the table are sent from the receiving port to all other ports. In the “Create static entry” dialog you can set up new filters. The following status settings are possible:

- ▶ `learned`: the filter was created automatically by the Switch.
- ▶ `invalid`: with this status you delete a manually created filter.
- ▶ `permanent`: the filter is stored permanently in the Switch or on the URL (see [“Saving settings” on page 57](#)).
- ▶ `gmrp`: the filter was created by GMRP.
- ▶ `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart.
- ▶ `igmp`: the filter was created by IGMP.

- ☐ To delete entries with the status “learned” from the filtering table select the `Basics:Restart` dialog and click on “Reset MAC address table”.

### 8.1.5 Disabling the specific packet distribution

To enable you to observe the data at all the ports, the Switch allows you to disable the learning of addresses. When the learning of addresses is disabled, the Switch transfers all the data from all ports to all ports.

- ☐ Select the `Switching:global` dialog.
- ☐ Checkmark “Address Learning” to observe the data of all ports.

## 8.2 Multicast application

### 8.2.1 Description multicast application

The data distribution in the LAN distinguishes between three distribution classes with reference to the addressed recipient:

- ▶ Unicast - one recipient
- ▶ Multicast - a group of recipients
- ▶ Broadcast - every recipient that can be reached

In the case of a Multicast address, Switches pass on all the data packets with a Multicast address to all the ports. This leads to an increased bandwidth requirement.

Protocols such as GMRP and processes such as IGMP Snooping enable the Switches to exchange information by means of the targeted distribution of Multicast data packets. The distribution of the Multicast data packets exclusively to those ports to which the recipients of these Multicast data packets are connected, reduces the bandwidth required.

You can recognize IGMP Multicast addresses by the area in which an address is located:

- ▶ MAC multicast address  
01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF
- ▶ IP multicast address class D  
224.0.0.0 - 239.255.255.255

### 8.2.2 Example of a multicast application

The cameras for machine surveillance normally transmit their images to monitor located in the machine room and in the monitoring room. In a IP transmission, a camera sends its image data with a multicast address over the network.

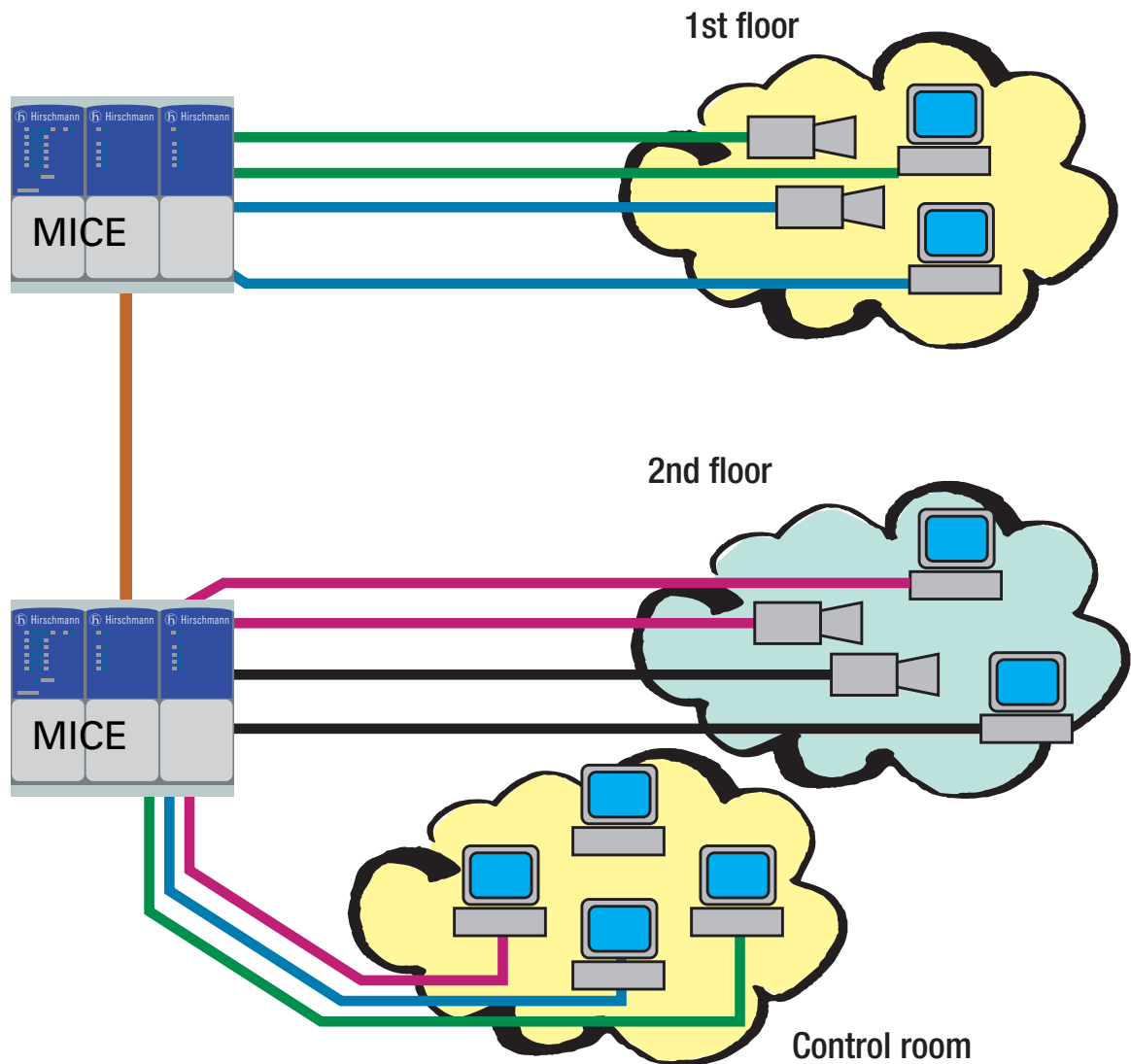


Fig. 33: Example: Video surveillance in machine rooms

### 8.2.3 Description IGMP snooping

The Internet **G**roup **M**anagement **P**rotocol (IGMP) describes the distribution of Multicast information between routers and terminal devices on the Layer 3 level.

Routers with an active IGMP function periodically send queries to find out which IP Multicast group members are connected to the LAN. Multicast group members reply with a Report message. This Report message contains all the parameters required by the IGMP. The router records the IP Multicast group address from the Report message in its routing table. The result of this is that it transfers frames with this IP Multicast group address in the target address field only in accordance with the routing table.


Devices which no longer want to be members of a Multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. In IGMP versions 1 and 2, the router removes the routing table entry if it does not receive any Report messages within a specified period of time (aging time).

If there are a number of routers with an active IGMP function in the network, then they work out among themselves which router carries out the Query function when using IGMP version 2. If there is no router in the network, then a suitably equipped Switch can carry out the Query function.

A Switch that connects a Multicast receiver with a router can evaluate the IGMP information with the aid of the IGMP Snooping procedure.

IGMP Snooping translates IP Multicast group addresses into MAC Multicast addresses, so that the IGMP functions can also be used by Layer 2 Switches. The Switch records the MAC addresses of the Multicast receivers, which are obtained by the IGMP Snooping from the IP addresses, in the static address table. Thus the Switch blocks Multicast packets at the ports at which no Multicast receivers are connected.

### 8.2.4 Setting multicast applications

- 
- ☐ Select the `Switching:Multicasts` dialog.



### ■ **Global Configuration**

With "IGMP Snooping" check box you can switch IGMP Snooping on/off globally for the entire Switch. If IGMP Snooping is switched off, then:

- ▶ the Switch does not evaluate Query and Report packets received and
- ▶ it sends (floods) received data packets with a Multicast address as the target address to all ports.

### ■ **IGMP Querier**

With "IGMP Querier active" you can switch the Query function on/off.

The Protocol check boxes allow you to select IGMP version 1, 2 or version 3.

### ■ **Unknown Multicasts**

"Send to Query Ports", the Switch sends the packets with an unknown MAC/IP multicast address to all query ports.

"Send to All Ports", the Switch sends the packets with an unknown MAC/IP multicast address to all ports.

"Discard", the Switch discards all packets with an unknown MAC/IP multicast address.

**Note:** The way in which unlearned multicast addresses are handled also applies to the reserved addresses from the "Local Network Control Block" (224.0.0.0 - 224.0.0.255). This can have an effect on the higher-level routing protocol.

### ■ **IGMP on per port**

This table column enables you to switch on/off the IGMP for each port when the global IGMP Snooping is switched on. When you switch off the IGMP at a port, no registrations can be made for this port.

### ■ **IGMP Forward All per port**

This column of the table allows you to switch on/off the IGMP Snooping function “Forward All” when the global IGMP Snooping is switched on. With the “Forward All” setting, the Switch forwards all the data packets with a Multicast address in the target address field to this port.

**Note:** If a number of routers are connected to a subnetwork, then you must use IGMP version 1, so that all the routers receive all the IGMP reports.

**Note:** If you use IGMP version 1 in a subnetwork, then you must also use IGMP version 1 in the entire network.

### ■ **Static Query Port**

A Switch sends IGMP report messages to the ports at which it receives IGMP queries. This column allows you to also send IGMP report messages to other selected ports.

### ■ **Learned Query Port**

A Switch sends IGMP report messages to the ports at which it receives IGMP queries. This column displays the ports on which the Switch has received IGMP queries.

**Note:** If the Switch is connected to a HIPER-Ring, in the case of a ring interruption you can ensure quick reconfiguration of the network for data packets with registered multicast target addresses by:

- ▶ switching on the IGMP at the ring ports and globally, and
- ▶ switching on the “IGMP Forward All” per port on the ring ports.

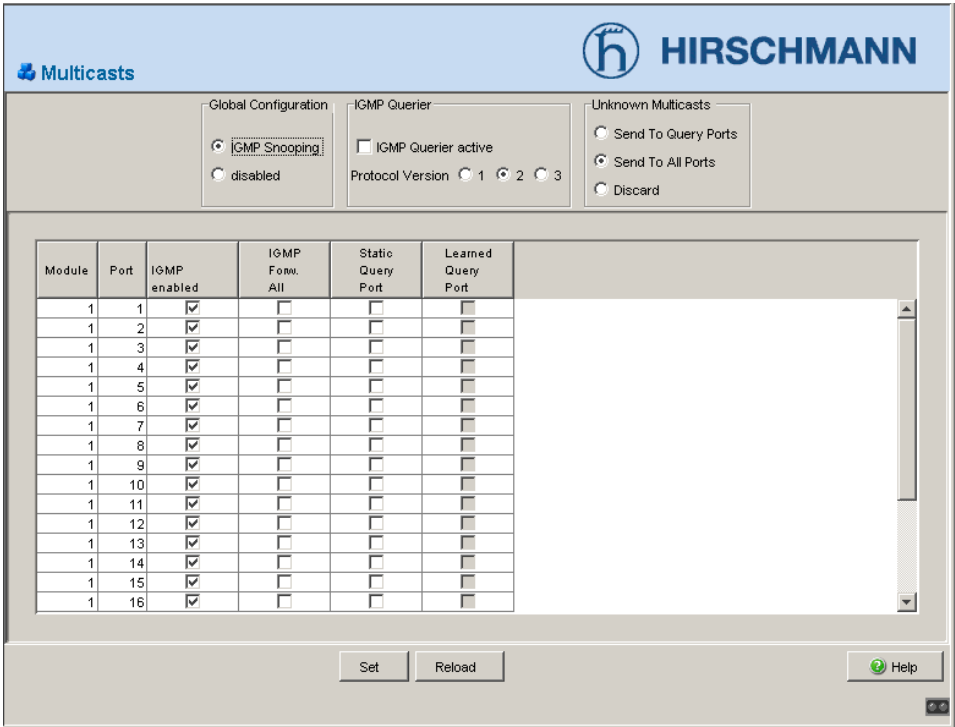


Fig. 34: IGMP dialog

## 8.3 Rate Limiter

### 8.3.1 Description Rate Limiter

To guarantee reliable data exchange during high traffic, the Switch can limit traffic.

Entering a limit rate for each port determines the amount of traffic the switch is permitted to transmit and receive.

If the data load transmitted on this port exceeds the maximum load, the Switch will discard the excessive data on this port.

A global setting activates/deactivates the rate limiter function at all ports.

### 8.3.2 Setting Rate Limiter for RS20/RS30/40, MS20/30, MACH 1000

- ☐ Select the `Switching:Rate Limiter` dialog.

With “Ingress Limiter” you can enable or disable the input limiting function for all ports.

With “Egress Limiter (p/s)” you can enable or disable the broadcast output limit on all ports.

With “Egress Limiter (kbit/s)” you can enable or disable the output limit for all packet types on all ports.

### Setting options per port:

- ▶ “Ingress Packet Types” offers the option of selecting the packet type(s) for which the limit is to apply:
  - ▶ All, limits all packets received at this port.
  - ▶ BC, limits only broadcast packets received at this port.
  - ▶ BC + MC, limits broadcast packets and multicast packets received at this port.
  - ▶ BC + MC + uUC, limits broadcast packets, multicast packets and unknown unicast packets received at this port.
- ▶ Ingress Limiter Rate for the selected packet type(s):
  - ▶ = 0, no ingress limit at this port.
  - ▶ > 0, maximum inbound traffic rate (in kbit/s) that is allowed to be received by and forwarded from this port.
- ▶ Egress Limiter rate for broadcast packets:
  - ▶ = 0, no rate limit for outbound broadcast packets at this port.
  - ▶ > 0, maximum broadcast rate that is sent on this port.
- ▶ Egress Limiter for all packet types:
  - ▶ = 0, no rate limit for outbound packets at this port.
  - ▶ > 0, maximum packet rate that is sent on this port.

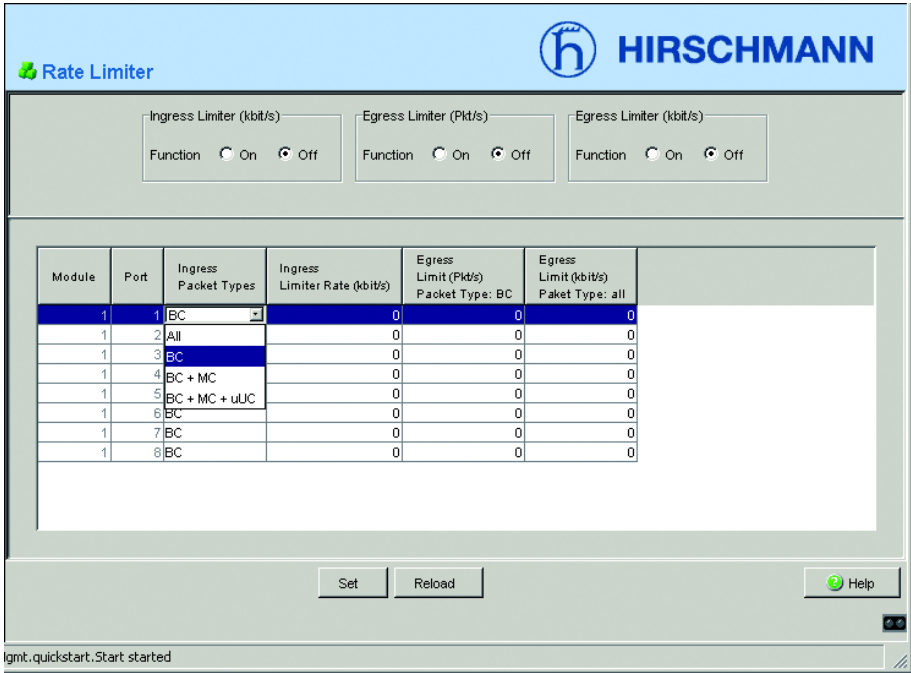


Fig. 35: Load limiter RS20/RS30/40, MS20/MS30, MACH 1000

## 8.4 Prioritization

### 8.4.1 Description Prioritization

This function prevents time-critical data traffic such as language/video or real time data from being disrupted by less time-critical data traffic during periods of heavy traffic. By assigning high priority classes for time-critical data and low priority classes for less time-critical data, you ensure optimal data flow for time-critical data traffic.

The Switch supports four priority queues (traffic classes in compliance with IEEE 802.1D-1998). The assignment of received data packets to these classes depends on

- ▶
- ▶ the priority of the data packet contained in the VLAN tag.
- ▶ the port priority for receiving the data packets that do not contain a tag (see [“Configuring ports” on page 69](#)).

Data packets can contain prioritizing/QoS information:

- ▶ VLAN priority based on IEEE 802.1Q/ 802.1D-1998 (Layer 2)

### 8.4.2 Tagging

The VLAN tag is integrated into the MAC data frame for the VLAN and prioritization functions in accordance with the IEEE 802.1 Q standard. The VLAN tag consists of 4 Bytes. It is inserted between the source address field and the type field.

With data packets with VLAN tag, the Switch evaluates

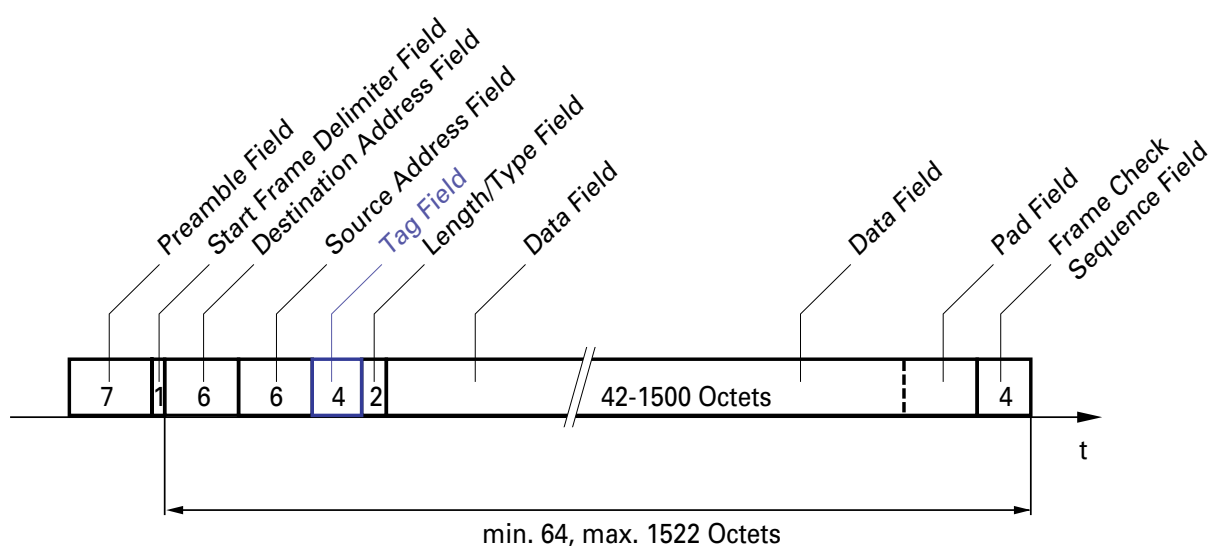
- ▶ the priority information at all times, and
- ▶ the VLAN information, if VLANs have been set up.

Data packets whose VLAN tags contain priority information but no VLAN information (VLAN ID = 0) are known as “Priority Tagged Frames”.

Entered priority	Priority class (default)	IEEE 802.1D traffic type
0	1	Best Effort (default)
1	0	Background
2	0	Standard
3	1	Excellent Effort (business critical)
4	2	Controlled load (streaming multimedia)
5	2	Video, less than 100 milliseconds of latency and jitter
6	3	Voice; less than 10 milliseconds of latency and jitter
7	3	Network Control reserved traffic

*Table 9: Assignment of the priorities listed in the tag to the four priority classes*

**Note:** Network logs and redundancy mechanisms use the highest priority classes 3 (RS20/30/40, MS20/30, MACH 1000, OCTOPUS) and 7 (Power MICE, MACH 4000). You therefore select other priority classes for application data.



*Fig. 36: Ethernet data packet with tag*



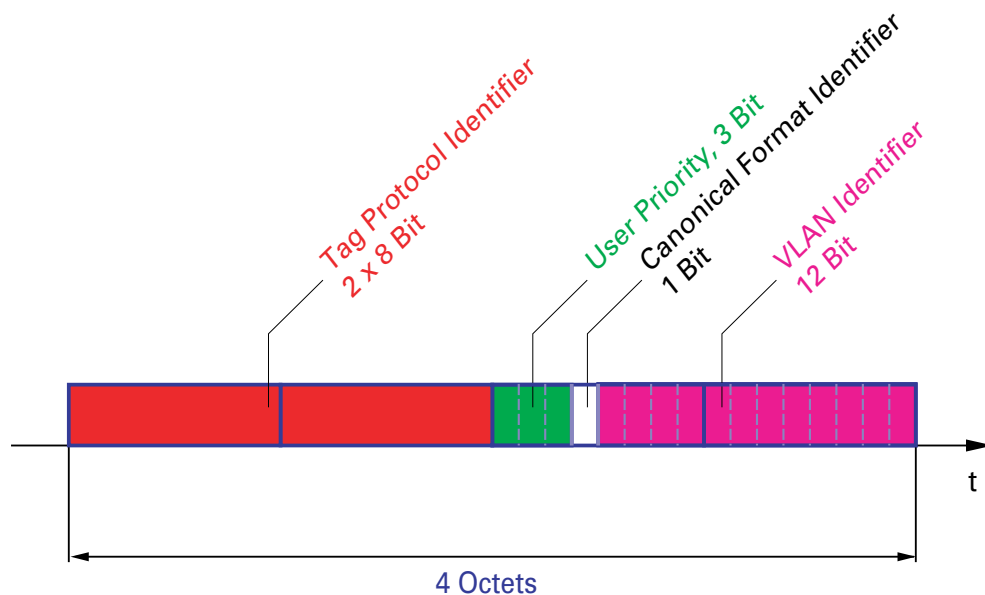


Fig. 37: Tag format

### 8.4.3 Handling of priority classes

For the handling of priority classes, the Switch provides:

- Strict priority

#### ■ Description Strict Priority

With Strict priority, the Switch sends all data packets with a higher priority level before it sends a data packet with the next lower priority level. Thus the Switch does not send a data packet with the next lower priority until there are no other data packets waiting in the queue. In some cases, a high level of data traffic can prevent packets with lower priority classes from being sent.

In applications that are time- or latency-critical, such as VoIP or video, this method ensures that high-priority data is sent immediately.

## 8.4.4 Setting Prioritization

- ☐ Select the `Basics:Port Configuration.dialog`.
- ☐ In the “Port Priority” column, you can specify the priority (0-7) with which the Switch sends data packets which it receives without a VLAN tag at this port.

**Note:** If you have set up VLANs, please observe the “Transparent Mode” under [“Configuring VLANs” on page 129](#).

### Setting the priority

```
enable
configure
interface 1/1

vlan priority 3
ex
```

Switch to the privileged EXEC mode.  
Switch to the configuration mode.  
Switch to the interface configuration mode for Interface 1/1.  
Assign the port priority 3 to the interface 1/1.  
Switch to the configuration mode.

### Assigning the VLAN priority to the priority classes

```
enable
configure
classofservice dot1p-map
ping 0 4
classofservice dot1p-map
ping 1 4
ex
show classofservice dot1p-
mapping
```

Switch to the privileged EXEC mode.  
Switch to the configuration mode.  
Assign the priority class 4 to the VLAN priority 0.  
  
Assign the priority class 4 to the VLAN priority 1.  
  
Switch to the privileged EXEC mode.  
Display the assignment.

```
show classofservice dot1p-mapping
```

User Priority	Traffic Class
-----	-----
0	4
1	4
2	1
3	3
4	4
5	5
6	6
7	7

## 8.5 Flow control

### 8.5.1 Description Flow control

Flow control is a mechanism which acts as an overload protection. During periods of heavy traffic it holds off additional traffic.

In the example (see fig. 38) the functioning of flow control is displayed graphically. Workstations 1, 2 and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2 and 3 is larger than the bandwidth of Workstation 4 to the Switch. This leads to an overflow of the send queue of Port 4. The left-hand funnel symbolizes this status.

If the flow control function at Ports 1, 2 and 3 of the Switch is turned on, the Switch reacts before the funnel overflows. Ports 1, 2 and 3 send a message to the connected devices that no data may be received at present.

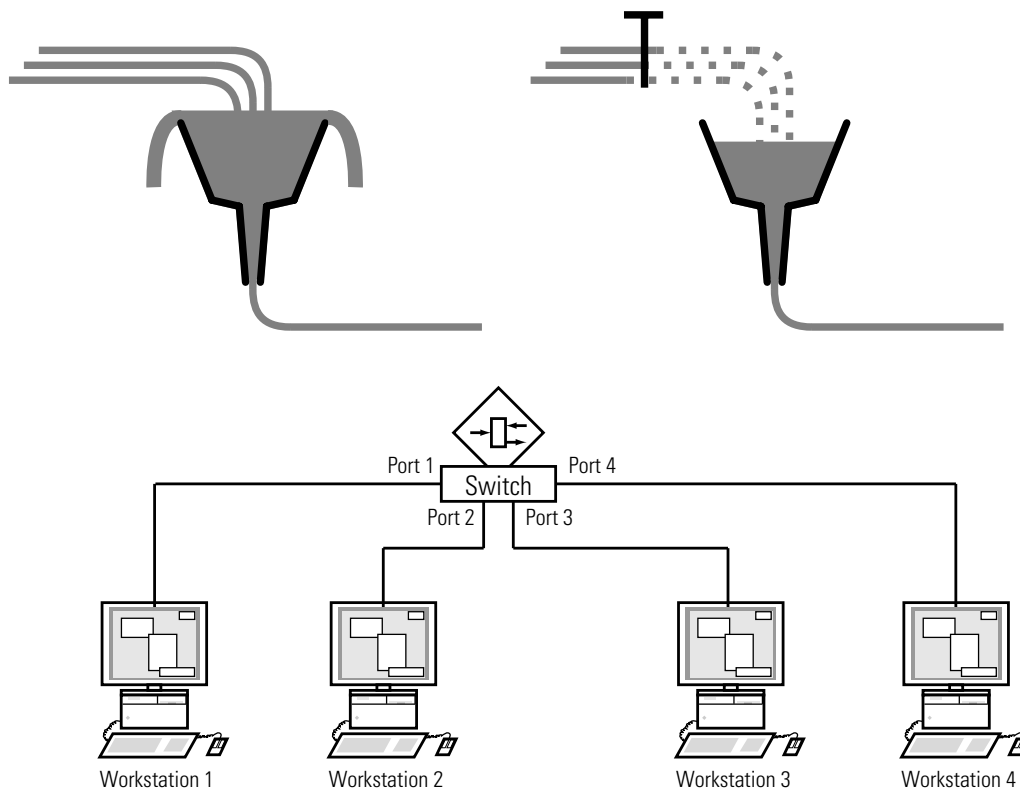


Fig. 38: Example of flow control

### ■ **Flow control with a full duplex link**

In the example (see fig. 38) there is a full duplex link between Workstation 2 and the Switch.

Before the send queue of Port 2 overflows, the Switch sends a request to Workstation 2 to include a small break in the sending transmission.

### ■ **Flow control with a half duplex link**

In the example (see fig. 38) there is a half duplex link between Workstation 2 and the Switch.

Before the send queue of Port 2 overflows, the Switch sends data so that workstation 2 detects a collision and thus interrupts the transmission.

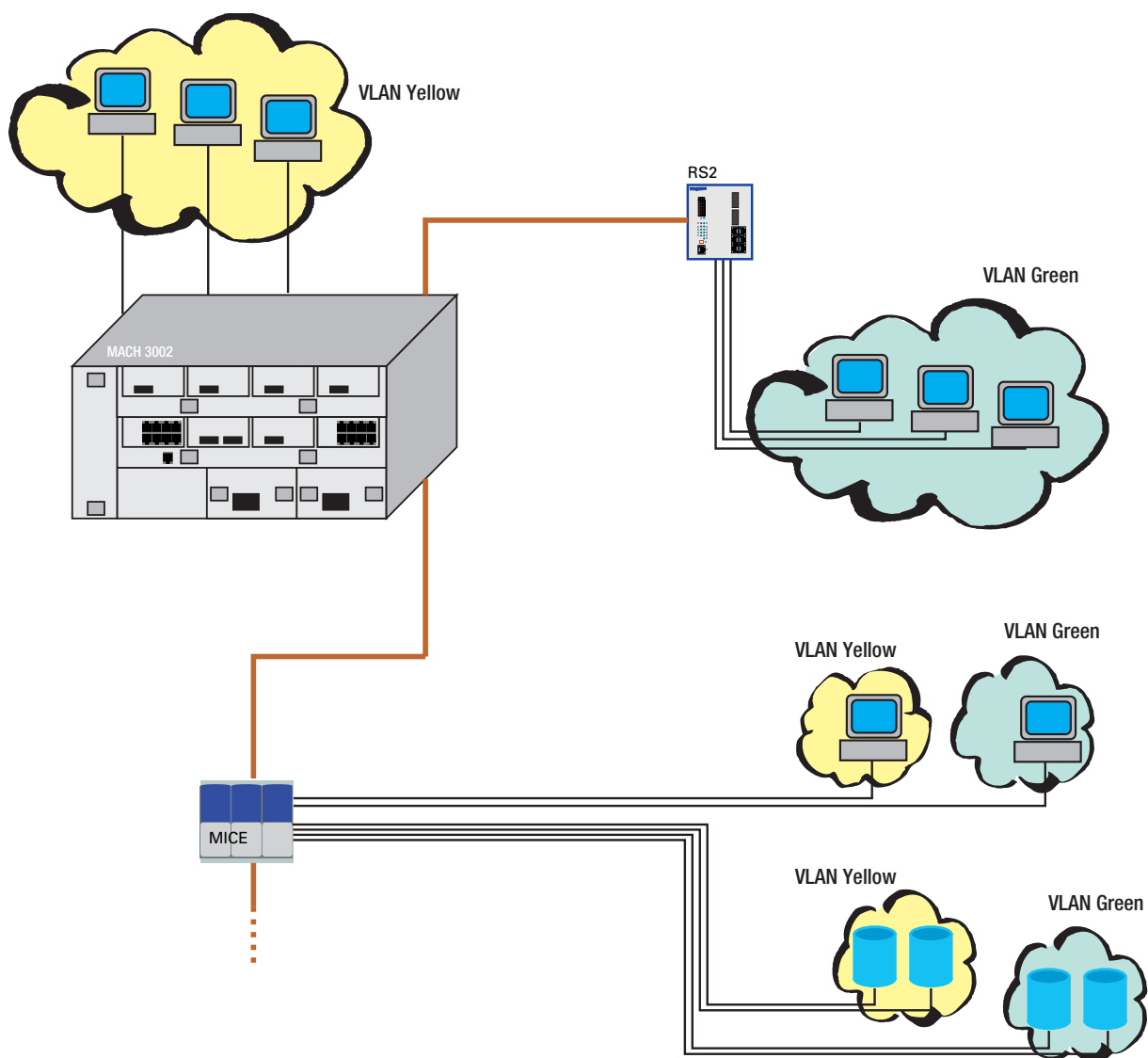
## 8.5.2 Setting flow control

- ☐ Select the `Basics:Port Configuration` dialog.  
In the “Flow Control” column, you mark this port to specify that flow control is active. Activate for this also the global switch “Flow Control” in the `Switching:Global` dialog.
- ☐ Select the `Switching:Global` dialog.  
This dialog enables you to
  - switch off flow control at all ports, or
  - switch on flow control at all ports which have been selected for flow control in the configuration table.

## 8.6 VLANs

### 8.6.1 Description VLANs

A virtual LAN (VLAN) consists of a group of network participants in one or more network segments who can communicate with each other as if they belonged to the same LAN.



*Fig. 39: Example of a VLAN*

VLANs are based on logical (instead of physical) links and are flexible elements in the network design. The biggest advantage of VLANs is the possibility of forming user groups based on the participant function and not on their physical location or medium.

Since broad/multicast data packets are transmitted exclusively within a virtual LAN, the remaining data network is unaffected.

The VLAN function is defined in the IEEE 802.1Q standard. The maximum number of VLANs is limited by the structure of the VLAN tag ([see fig. 37](#)) to 4094.

Key words often used in association with VLANs are:

#### ■ **Ingress Rule**

The ingress rules stipulate how incoming data is to be handled by the Switch.

#### ■ **Egress Rule**

The egress rules stipulate how outgoing data is to be handled by the Switch.

#### ■ **VLAN identifier**

The assignment to a VLAN is effected via a VLAN ID. Every VLAN existing in a network is identified by an ID. This ID must be unique, i.e. every ID may only be assigned once in the network.

#### ■ **Port VLAN identifier (PVID)**

The management assigns a VLAN ID for every port. It is known, therefore, as the port VLAN ID.

The Switch adds a tag to every data packet received with no tag. This tag contains a valid VLAN ID.

When a data packet is received with a priority tag the Switch adds the port VLAN ID.

**■ Member set**

The member set is list of ports belonging to a VLAN. Every VLAN has a member set.

**■ Untagged set**

The untagged set is a list of the ports of a VLAN which send data packets without a tag. Every VLAN has an untagged set.



## 8.6.2 Configuring VLANs

- ☐ Select the `Switching:VLAN` Dialog.

Under VLAN you will find all tables and attributes to configure and monitor the VLAN functions complying with IEEE 802.1Q standard.

- ☐ Select the dialog `Switching:VLAN:Global`.
- ☐ Activate “VLAN Transparent Mode” to transmit priority-tagged packets that are not a member of a VLAN, i.e. have a VLAN-ID of “0”. In this mode the VLAN-ID “0” is retained in the packet, regardless of the setting of the port VLAN ID in the “VLAN Port” dialog.

**Note:** For RS20/RS30/RS40, MS20/MS30, MACH 1000 and OCTOPUS In “transparent mode”, the devices ignore the set port VLAN-ID. Set the VLAN membership of the ports of VLAN 1 to `member` or `untagged`.

### Note:

**Note:** When configuring the VLAN, ensure that the port to which your management station is connected, can still send the data of the management station after saving the VLAN configuration. Assigning the port to the VLAN with ID 1 always ensures that the management station data can be sent.

After changing entries:

`Set`

The agent saves the new entry.

The modification will take effect immediately.

`Reload`

Displays the updated configuration.

**Note:** Save the VLAN configuration to non-volatile memory (see fig. 45).

**Note:** The 256 available VLANs can use any VLAN ID in the range 1 to 4042.

**Note:** In a HIPER-Ring with VLANs you should only operate devices with the software that supports this function, namely:

- ▶ RS2 xx/xx (from Vers. 7.00),
- ▶ RS2-16M,
- ▶ RS 20, RS 30, RS 40
- ▶ MICE (from Rel. 3.0) or
- ▶ Power MICE
- ▶ MS 20, MS 30
- ▶ MACH 1000
- ▶ MACH 3000 (from Rel. 3.3)
- ▶ MACH 4000
- ▶ OCTOPUS

**Note:** In the HIPER-Ring configuration, select for the ring ports

- VLAN ID 1 and “Ingress Filtering” disabled in the port table and
- VLAN affiliation  $\cup$  in the static table.

**Note:** In the Ring/Network Coupling configuration, select for the coupling and partner coupling ports

- VLAN ID 1 and “Ingress Filtering” disabled in the port table and
- VLAN affiliation  $\cup$  in the static table.

### 8.6.3 Setting up VLANs

- ☐ Select the `Switching:VLAN:Static` dialog.

To set up VLANs, you first specify the desired VLANs in the VLAN static table:

- ☐ After clicking on “Create”, you enter the appropriate VLAN ID. A new line appears in the table.
- ☐ Enter the name of your choice for this VLAN.
- ☐ Define the affiliation of the ports you require.
  - not a member of the VLAN.
  - M a member of the VLAN - packet is transmitted with tag .
  - F not a member of the VLAN
  - U a member of the VLAN - packet is transmitted without tag.
- ☐ After setting up VLANs, you specify the rules for received data in the VLAN Port table (port):
  - ▶ Port VLAN ID  
specifies to which VLAN a received untagged data packet is assigned.
  - ▶ Acceptable Frame Types  
determines if data packets can also be received untagged.
  - ▶ Ingress Filtering  
specifies whether the received tags are evaluated.

### 8.6.4 Displaying the VLAN configuration

- ☐ Select the `Switching:VLAN:Current` dialog.  
The `Current` table displays all locally configured VLANs.

## 8.6.5 Deleting the VLAN settings

- ☐ Select the `Switching:VLAN:Global` dialog.  
The “Delete” button in the VLAN global dialog allows you to restore all the default VLAN settings of the device (state on delivery).
- ☐ Select the `Switching:VLAN:Static` dialog.  
The “Delete” button in the VLAN static dialog allows you to delete a selected row of the table.

### 8.6.6 Example of a simple VLAN

The following example provides a quick insight into configuring a VLAN that is commonly found in practice.

The configuration is explained step by step.

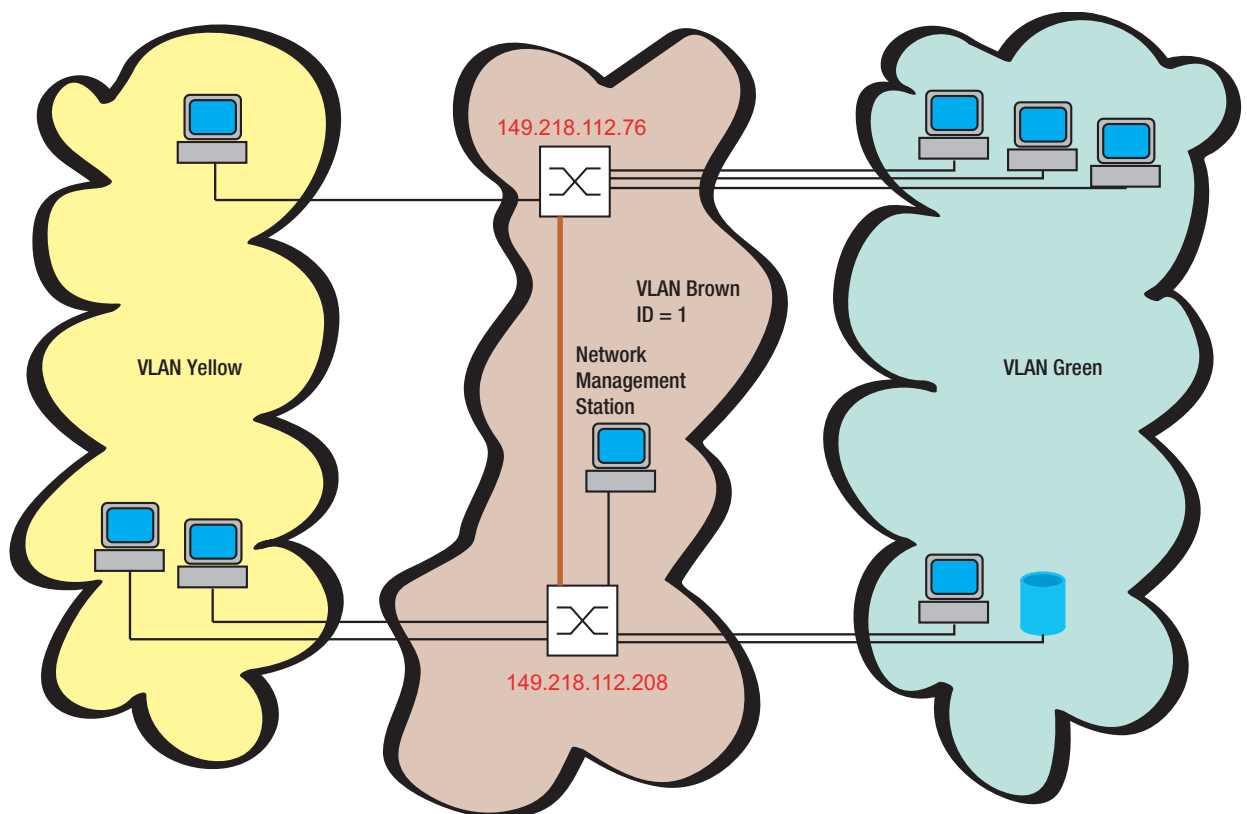


Fig. 40: Example of a VLAN

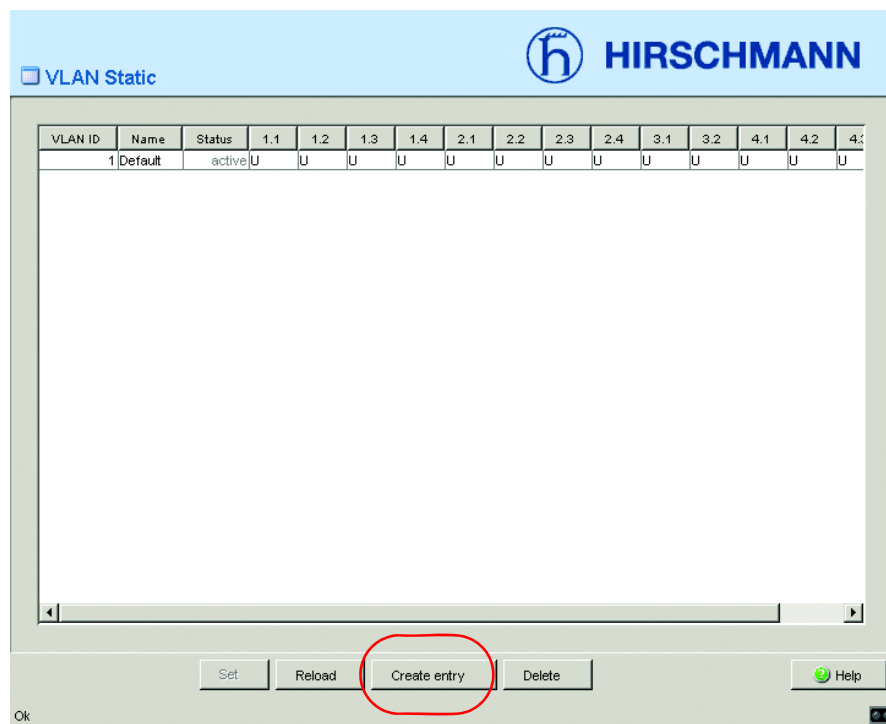


Fig. 41: Creating a VLAN

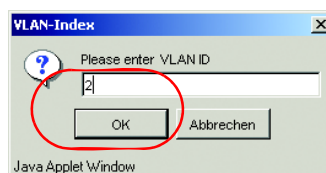


Fig. 42: Entering a VLAN ID

- ☐ Repeat the steps: Creating a VLAN and Entering a VLAN ID for all VLANs.

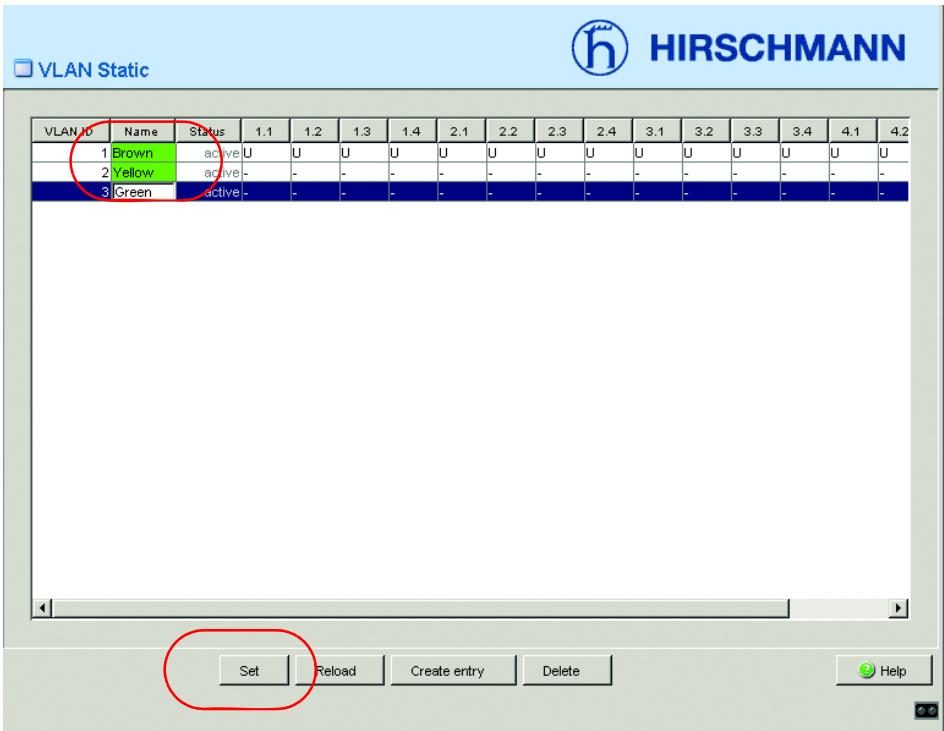


Fig. 43: Assigning a VLAN any name and saving it

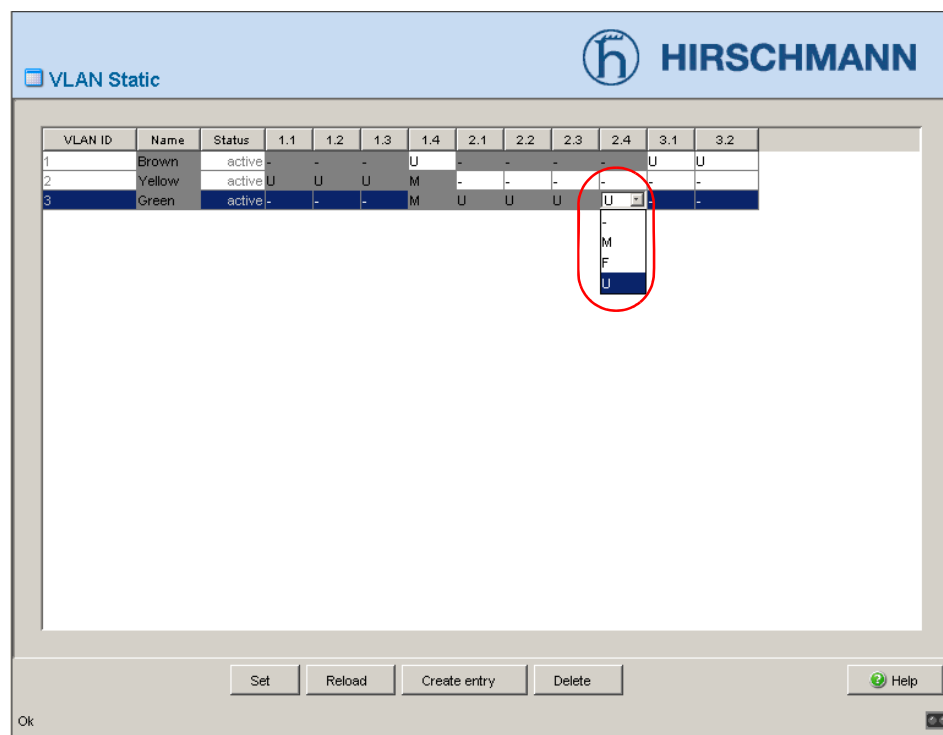


Fig. 44: Defining the VLAN membership of the ports.

Ports 1.1 to 1.3 are assigned to the terminal devices of the yellow VLAN and ports 2.1 to 2.4 to the terminal devices of the green VLAN. As terminal devices normally do not send data packets with a tag, the setting **U** must be selected here.

Port 1.4 serves as uplink port to the next Switch. It is assigned the setting **M**. The VLAN information can thus be passed on.



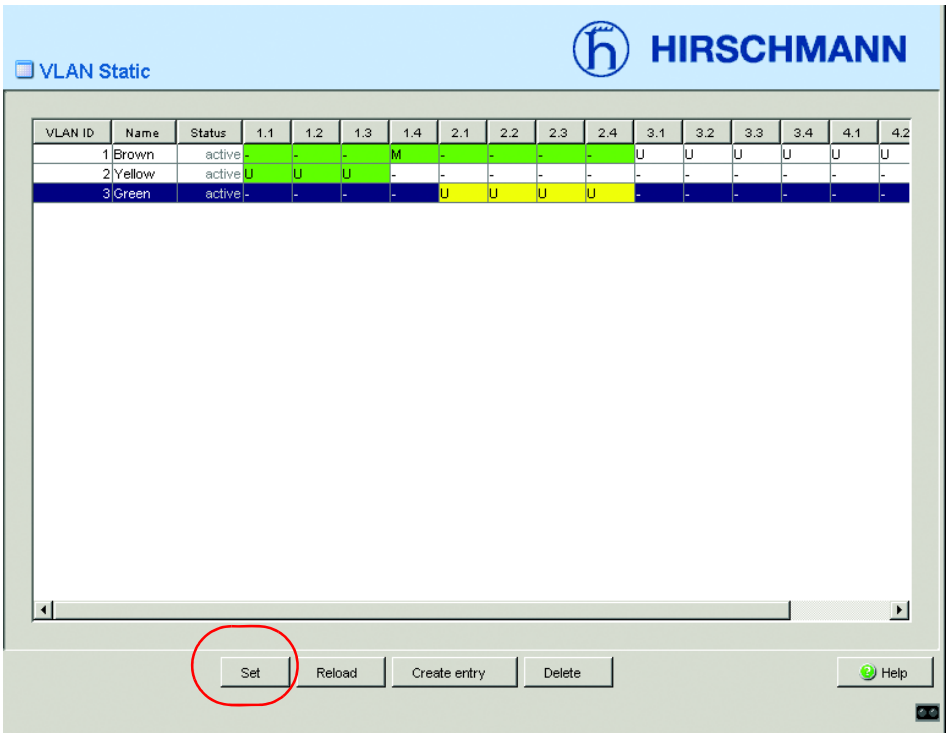


Fig. 45: Saving the VLAN configuration

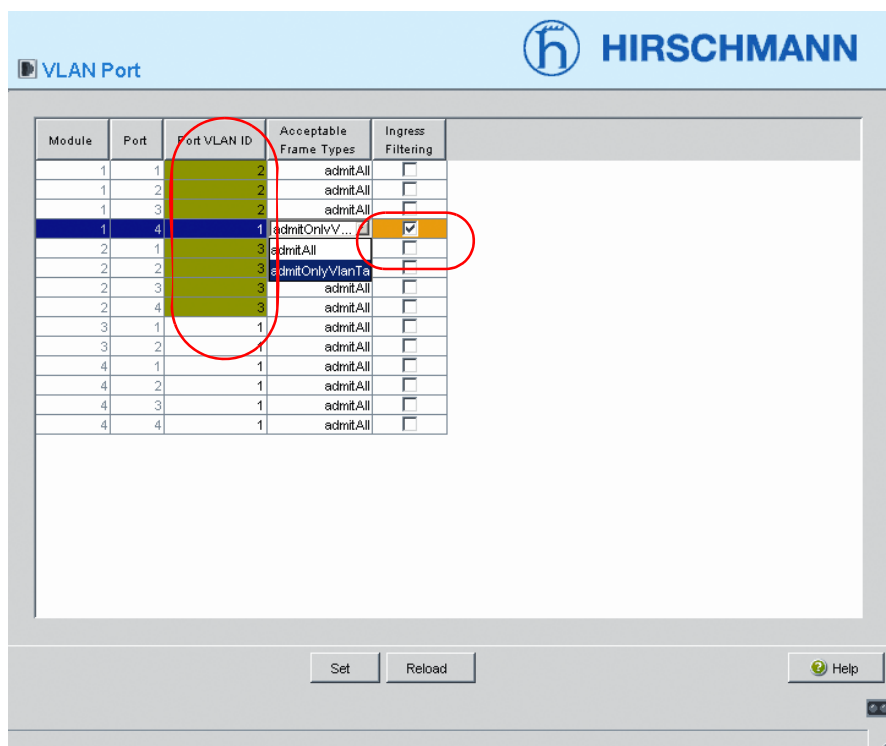



Fig. 46: Assigning the VLAN ID, Acceptable Frame Types and Ingress Filtering to the ports and saving it

Ports 1.1 to 1.3 are assigned to the terminal devices of the yellow VLAN and therefore VLAN ID 2 and ports 2.1 to 2.4 are assigned to the terminal devices of the green VLAN and hence VLAN ID 3. Because terminal devices usually do not send data packets with a tag, you select the `admitAll` setting here.

Port 1.4 serves as an uplink port to the next Switch. It belongs to the brown VLAN and is thus given the VLAN ID 1. It is assigned the setting `admitOnlyVlanTagged`. Thus only packets with a VLAN tag can be received by this port.

Activating the `Ingress Filter` ensures that the tags received at the port are evaluated.

**Load/Save**  **HIRSCHMANN**

**Load**

☒ from Switch ☐ from URL ☐ from URL & save to Switch ☐ via PC (script / binary)

**Save**

☒ to Switch ☐ to URL (binary) ☐ to URL (script) ☐ to PC (binary) ☐ to PC (script)

URL:

**Delete**

☒ current configuration ☐ current configuration and from Switch

**AutoConfiguration Adapter**

Status:

**Undo modifications of configuration**

Function ☐ Period to undo while connection is lost [s]

*Fig. 47: Saving the configuration to non-volatile memory*



## 9 Operation Diagnostics

The Switch provides you with the following diagnostic tools for the function diagnosis:

- ▶ Sending traps
- ▶ Monitoring Device Status
- ▶ Out-of-band signaling via signal contact
- ▶ Port status indication
- ▶ Event counter on port level
- ▶ SFP status indication
- ▶ Topology discovery
- ▶ Reports
- ▶ Monitoring the traffic of a port (Portmirroring)

## 9.1 Sending traps

If unusual events occur during normal operation of the Switch, they are reported immediately to the management station. This is done by means of so-called **traps** - alarm messages - that bypass the polling procedure ("Polling" means querying the data stations at regular intervals). Traps make it possible to react quickly to critical situations.

Examples of such events are:

- ▶ a hardware reset
- ▶ changing the basic device configuration
- ▶ segmentation of a port
- ▶ ...

Traps can be sent to various hosts to increase the transmission reliability for the messages. A trap message consists of a packet that is not acknowledged.

The Switch sends traps to those hosts that are entered in the trap destination table. The trap destination table can be configured with the management station via SNMP.

### 9.1.1 SNMP trap listing

All possible traps that can occur are listed in the following table.

Trap description	Meaning
authenticationFailure	is sent if a station attempts to access an agent without permission.
coldStart	is sent for a cold and warm start during the boot process after successful management initialization.
hmAutoconfigAdapterTrap	is sent when the ACA AutoConfiguration Adapter is inserted or removed.
linkDown	is sent if the link to a port is interrupted.
linkUp	is sent if the link to a port is re-established.
hmTemperature	is sent if the temperature exceeds the limit set.
hmPowerSupply	is sent if the status of the voltage supply changes.
hmSigConRelayChange	is sent if the status of the signal contact changes.
newRoot	is sent if the sending agent becomes the new root of the spanning tree.
topologyChange	is sent if the transmission mode of a port changes.
risingAlarm	is sent if an RMON alarm input exceeds the upper threshold.
fallingAlarm	is sent if an RMON alarm input falls below the lower threshold.
hmPortSecurityTrap	is sent if a MAC address is detected at the port which does not correspond to the current settings of: – hmPortSecPermission and – hmPortSecAction set either to trapOnly (2) or portDisable (3)
hmModuleMapChange	is sent, if the hardware configuration has changed.
hmBPDUGuardTrap	is sent if a BPDU is received at a port although the BPDU guard function is activated.
hmMrpReconfig	is sent if the configuration of the MRP ring changes.
hmRingRedReconfig	is sent if the configuration of the HIPER ring changes.
hmRingRedCplReconfig	is sent if the configuration of the redundant ring/network coupling changes.
hmSNTPTrap	is sent if errors occur in connection with the SNTP protocol (e.g. server not available).
hmRelayDuplicateTrap	is sent if a duplicate IP address is detected in connection with the DHCP Option 82.
lldpRemTablesChangeTrap	is sent if an entry in the topology table changes.

*Table 10: Possible traps*

## 9.1.2 SNMP traps when booting

The ColdStart trap is sent during every boot procedure.

## 9.1.3 Configuring traps

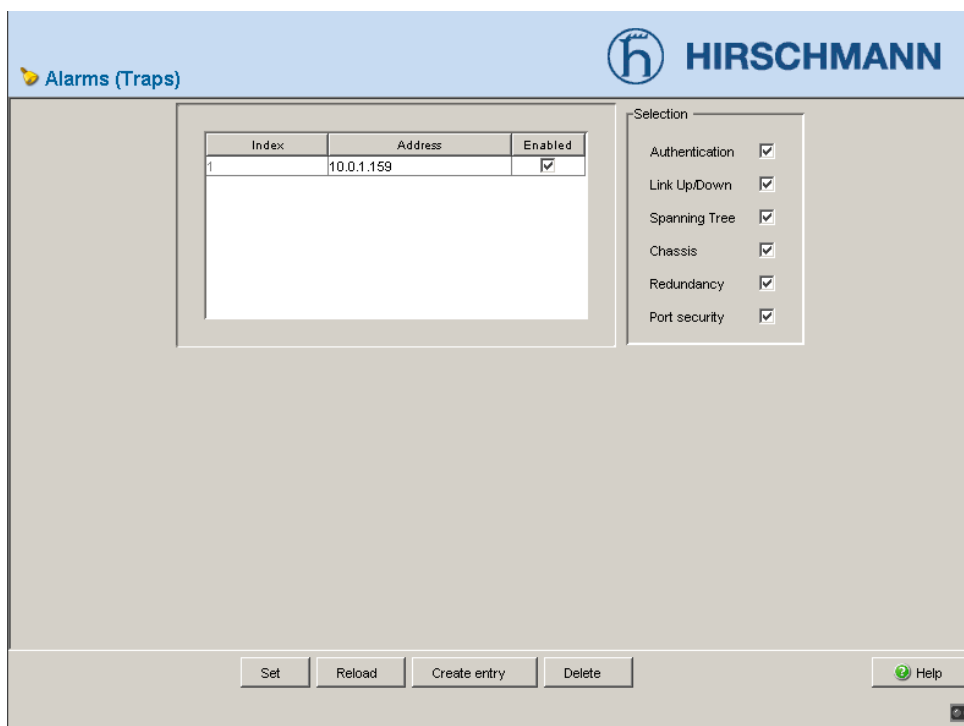
- ☐ Select the `Diagnostics:Alarms (Traps)` dialog.

This dialog allows you to specify which events trigger an alarm (trap) and to whom these alarms should be sent.

- ☐ In the “IP Address” column, enter the IP address of a network management station to which the traps should be sent.
- ☐ In the “Active” column, you mark the entries which should be taken into account when traps are being sent.
- ☐ In the frame “Selection” select these trap categories from which you want to send traps

**Note:** Access this dialog with read-write password.





*Fig. 48: Alarmes dialog*

The events which can be selected are:

Name	Bedeutung
Authentication	The Switch has rejected an unauthorized access attempt (see the Access for IP Addresses und Port Security dialog).
Cold Start	The Switch has been switched off.
Link Down	At one port of the Switch, the link to the device connected there has been interrupted.
Link up	At one port of the Switch, the link to a device connected there has been established.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.

*Table 11: Trap categories*

Name	Bedeutung
Chassis	<p>encompasses the following events:</p> <ul style="list-style-type: none"> <li>– Power Supply: The status of a supply voltage has changed (see the <code>System</code> dialog).</li> <li>– Signaling Relay: The status of the signal contact has changed. To consider this event enable “generate Trap” in the <code>Diagnostics:Signal Contact 1/2</code> Dialog.</li> <li>– An error has occurred in connection with the SNTP.</li> <li>– A media module has been added or removed.</li> <li>– The AutoConfiguration Adapter, ACA, has been inserted or removed.</li> <li>– The value exceeded / fell below the temperature threshold.</li> </ul>
Redundancy	The status of the HIPER-Ring or the redundant coupling of HIPER-Rings / network segments has changed.
Port Security	On one port a data packet has been received from an unauthorized terminal device (see <code>Port Security</code> Dialog).
Bridge	Although the BPDU guard function is activated at a port a BPDU was received (see User Manual Redundancy under „Rapid Spanning Tree“).

Table 11: Trap categories

## 9.2 Monitoring Device Status

The device status provides an overview of the overall condition of the Switch. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

The Switch enables you to

- ▶ signal the device status out-of-band via a signal contact (see [“Monitoring the Device Status with a signal contact” on page 153](#)).
- ▶ signal the device status by sending a trap when the device status changes.
- ▶ detect the device status in the Web-based interface on the system side.
- ▶ query the device status in the Command Line Interface.

The device status of the Switch includes:

- ▶ Incorrect supply voltage, the failure of at least one of the two supply voltages or a permanent fault in the Switch (internal supply voltage).
- ▶ The temperature threshold has been exceeded or has not been reached.
- ▶ Removing a module (at modular devices).
- ▶ Removing the ACA.
- ▶ Failure of a fan (MACH 4000).
- ▶ The defective link status of at least one port. With the Switch, the indication of link status can be masked by the management for each port (see [“Displaying connection error messages” on page 70](#)). Link status is not monitored in the delivery condition.
- ▶ HIPER-Ring event: the loss of redundancy guarantee (in Redundancy Manager mode). Ring redundancy is not monitored in the delivery condition.
- ▶ Redundant Ring/Netcoupling event: the loss of redundancy guarantee. Ring redundancy is not monitored in the delivery condition.  
In Stand-by mode the Switch reports additionally the following conditions:
  - the faulty link status of the control line
  - partner device is in stand-by mode

It depends on the management setting which events cause a contact to switch.

**Note:** With non-redundant supply of the mains voltage, the Switch reports a power failure. You can prevent this message by applying the supply voltage over the two inputs or by switching off the monitoring (see [“Monitoring correct operation via the signal contact” on page 152](#)).

- ☐ Select the `Diagnostics:Device Status`.
- ☐ Select in the frame “Monitoring correct operation” the events which you want to have monitored.
- ☐ For temperature monitoring set in the `Basics: System` dialog at the end of the system data the temperature thresholds..

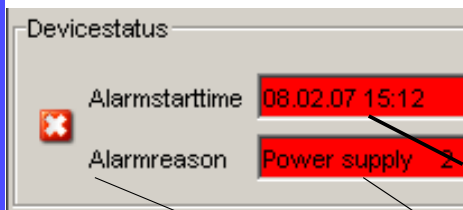
Configure Device Status

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the configuration mode.
<code>device-status monitor all enable</code>	Includes all the possible events in the device status determination.
<code>device-status trap enable</code>	Enables a trap to be sent if the device status changes.

Display Device Status

<code>exit</code>	Switch to the privileged EXEC mode.
<code>show device-status</code>	Displays the device status and the setting for the device status determination.

- ☐ Select the Basics: System dialog.



Time of the oldest existing alarm

Cause of the oldest existing alarm

Symbol indicates the Device Status

*Fig. 49: Device Status display*

## 9.3 Out-of-band signaling

The signal contacts are for

- ▶ controlling external devices by manually setting the signal contacts.
- ▶ monitoring proper functioning of the Switch which makes it possible to perform remote diagnostics.

A break in contact is reported via the potential-free signal contact (relay contact, closed circuit):

- ▶ Faulty power supply:  
the failure of the supply voltage 1/2,  
a continuous malfunction in the Switch (internal supply voltage).
- ▶ Values that exceed or fall below the set temperature threshold.
- ▶ Removing a module.
- ▶ Removing the ACA.
- ▶ The defective link status of at least one port. With the Switch, the indication of link status can be masked by the management for each port (see [“Displaying connection error messages” on page 70](#)). Link status is not monitored in the delivery condition.
- ▶ HIPER-Ring event:  
the loss of redundancy guarantee (in Redundancy Manager mode). Ring redundancy is not monitored in the delivery condition.
- ▶ Redundant Ring/Netcoupling event:  
the loss of redundancy guarantee. Ring redundancy is not monitored in the delivery condition.  
In Stand-by mode the Switch reports additionally the following conditions:
  - the faulty link status of the control line
  - partner device is in stand-by mode

It depends on the management setting which events cause a contact to switch.

**Note:** With non-redundant supply of the mains voltage, the Switch reports a power failure. You can prevent this message by applying the supply voltage over the two inputs or by switching off the monitoring (see [“Monitoring correct operation via the signal contact” on page 152](#)).

### 9.3.1 Manual setting the signal contact

This mode gives you the option of remote switching each signal individually.

Application options:

- ▶ Simulation of an error during SPS error monitoring.
- ▶ Remote control of a device via SNMP, such as switching on a camera..

- ☐ Select the `Diagnostics:Signal Contact 1/2` dialog.
- ☐ Select “Manual setting” in the “Mode Signal Contact” frame, to switch the contact manually.
- ☐ Select “Opened” in the “Manual setting” frame to open the contact.
- ☐ Select “Closed” in the “Manual setting” frame to close the contact.

#### Configure signal contact

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the configuration mode.
<code>signal-contact 1 mode manual</code>	Selects the manual setting mode for signal contact 1.
<code>signal-contact 1 state open</code>	Opens signal contact 1.
<code>signal-contact 1 state closed</code>	Closes signal contact 1.

## 9.3.2 Monitoring correct operation via the signal contact

### ■ Configuring the monitoring correct operation

- ☐ Select the `Diagnostics:Signal Contact` dialog.
- ☐ Select “Monitoring correct operation” in the frame “Mode Signal contact”, to use the contact for function monitoring.
- ☐ Select in the frame “Monitoring correct operation” the events which you want to have monitored.
- ☐ For temperature monitoring set in the `Basics:System` dialog at the end of the system data the temperature thresholds..

### Configuring the monitoring correct operation

<code>enable</code>	Switch to the privileged EXEC mode.
<code>configure</code>	Switch to the configuration mode.
<code>signal-contact 1 monitor all</code>	Includes all the possible events in the function monitoring.
<code>signal-contact 1 trap enable</code>	Enables a trap to be sent if the status of the function monitoring changes.

### ■ Signal contact display

You can view the signal contact status in three ways:

- ▶ using the LED display,
- ▶ using the web-based interface,
- ▶ executing a query in the command line interface.



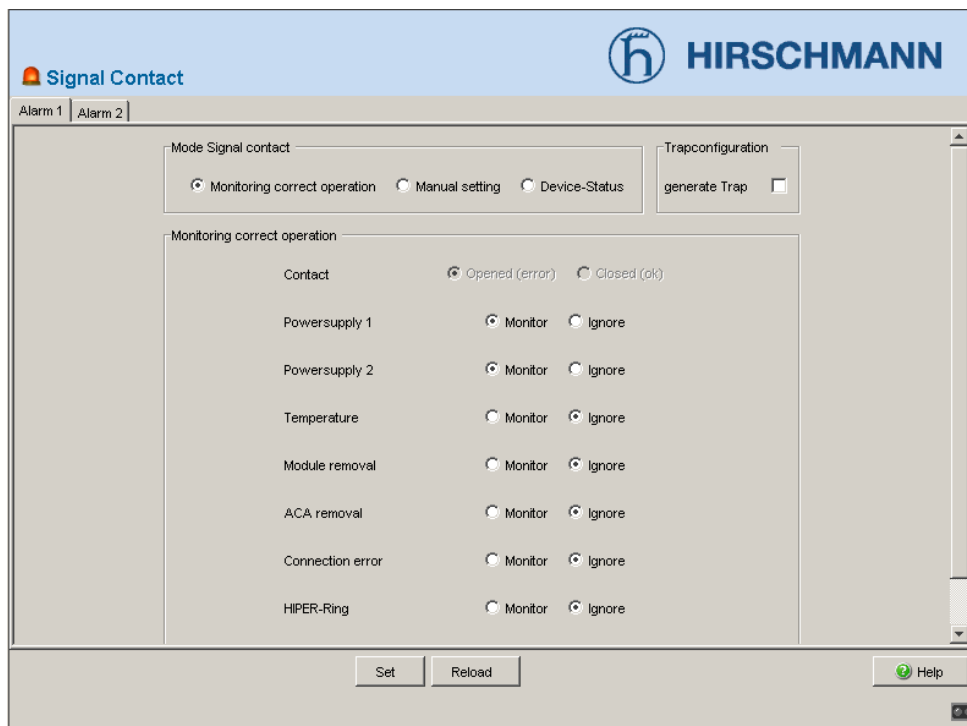


Fig. 50: Signal contact dialog

### Display signal contact status

```
exit
show signal-contact 1
```

Switch to the privileged EXEC mode..  
Displays the status of the function monitoring and the setting for the status determination.

## 9.3.3 Monitoring the Device Status with a signal contact

The “Device status” option enables you, like in the function monitoring, to monitor the device status (see [“Monitoring Device Status” on page 147](#)) via the signal contact.

## 9.4 Port status indication

- ☐ Select the `Basics:System` dialog.

The device view displays the Switch with the current configuration. The symbols underneath the device view represent the status of the individual ports.

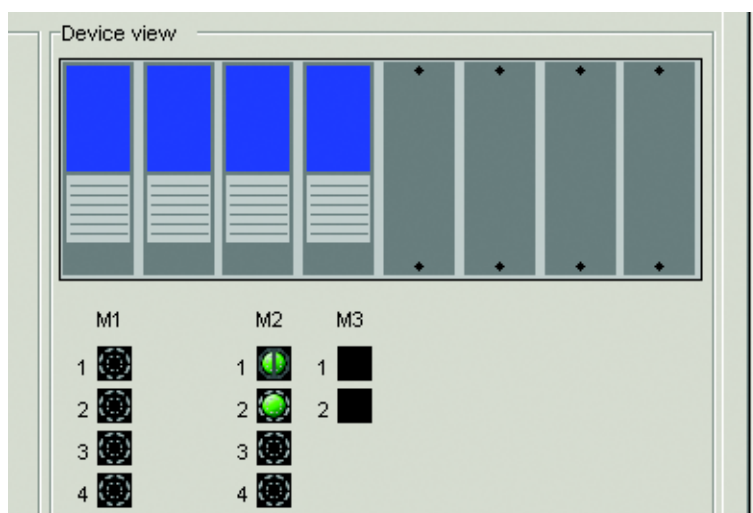







Abb. 51: Example for a device view

Meaning of the symbols:

-  The port (10, 100, 1000 MBit/s) is enabled and the connection is OK.
-  The port is locked by management.
-  The port is in FDX mode.
-  The port is in HDX mode.
-  The port is in RSTP discarding mode.



The port is in autonegotiation mode.

## 9.5 Event counter on port level

The port statistics table allows experienced network administrators to identify possible problems occurring in the network.

This table shows you the contents of various event counters. In the menu item restart with "Restart Switch", "Hot restart" or "Reset port counters" you can reset all event counters to zero.


The counters add up the events transmitted and the events received.

Counter	Possible Problems
Received Fragments	<ul style="list-style-type: none"> <li>– The controller of the connected device is faulty.</li> <li>– Electromagnetic interference is injected into transfer medium.</li> </ul>
CRC error	<ul style="list-style-type: none"> <li>– The controller of the connected device is faulty.</li> <li>– Electromagnetic interference is injected into transfer medium - there is a faulty component in the network.</li> </ul>
Collisions	<ul style="list-style-type: none"> <li>– The controller of the connected device is faulty.</li> <li>– The network expansion is too big or the line is too long.</li> <li>– A packet has collided with an interference signal.</li> </ul>

*Table 12: Examples indicating possible problems*

- ☐ Select the `Diagnostics:Ports:Statistics` dialog.
- ☐ For resetting port counters select "Reset port counters" in the `Basics:Restart` dialog.

Statistics Table

 **HIRSCHMANN**

Module	Port	Transmitted Unicast Packets	Received Packets	Received Octets	Received Fragments	Detected CRC errors	Detected Collisions	Packets 64 bytes	Packets 65 to 127 bytes
1	1	0	0	0	0	0	0	0	0
1	2	0	0	0	0	0	0	0	0
1	3	0	0	0	0	0	0	0	0
1	4	0	0	0	0	0	0	0	0
2	1	111084	137980	21276544	0	0	310	74445	36
2	2	87	55387	5445592	0	0	0	70079	3
2	3	0	0	0	0	0	0	0	0
2	4	0	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0	0	0
3	2	0	0	0	0	0	0	0	0

Reload


 Help

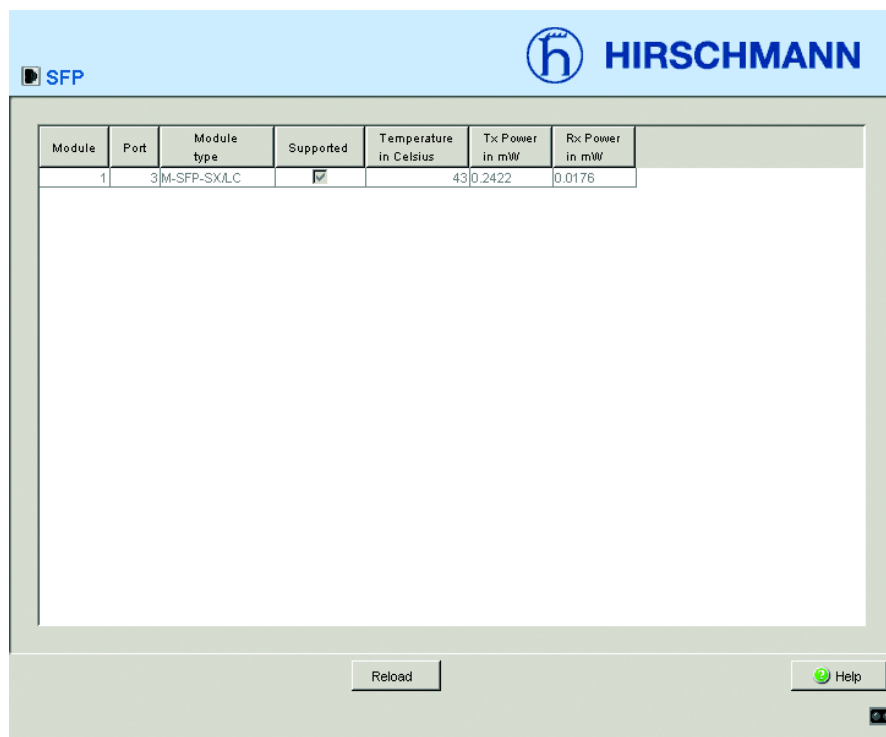
Fig. 52: Port statistic table

## 9.6 Displaying the SFP Status

By having the SFP status displayed you can view the current connection to the SFP modules and their properties. The properties include:

- ▶ module type,
- ▶ support provided in the media module
- ▶ temperature in degrees Celsius
- ▶ transmission power in milliwatts
- ▶ reception power in milliwatts

☐ Select the `Diagnostics:Ports:SFP` modules dialog.



Module	Port	Module type	Supported	Temperature in Celsius	Tx Power in mW	Rx Power in mW
1	3	M-SFP-SX/LC	<input checked="" type="checkbox"/>	43	0.2422	0.0176

Fig. 53: SFP modules dialog

## 9.7 Topology discovery

### 9.7.1 Description Topology discovery

IEEE 802.1AB describes the Link Layer Discovery Protocol (LLDP). LLDP allows users to automatically detect the topology of their LANs.

A device with active LLDP

- ▶ sends its own connection and management information to neighboring devices of the shared LAN, in as far as they have also LLDP activated.
- ▶ receives connection and management information from neighboring devices of the shared LAN, in as far as they have also LLDP activated.
- ▶ sets up a management information scheme and object definitions for saving connection information of neighboring devices that have LLDP activated.

The connection information contains as its most significant element the precise and unique ID of a connection endpoint: MSAP (MAC Service Access Point). This is composed of the MAC address of the device and a port ID that is unique to this device.

Contents of the connection and management information:

- ▶ Chassis ID (its MAC address)
- ▶ Port ID (its port MAC address)
- ▶ Description of the port
- ▶ System name
- ▶ System description
- ▶ Supported “system capabilities” (e.g. router = 14 or switch = 4)
- ▶ Currently activated “system capabilities”
- ▶ Interface ID of the management address
- ▶ VLAN-ID of the port
- ▶ Status of autonegotiation on the port
- ▶ Medium, half/full duplex setting and transmission speed setting of the port
- ▶ Information about the redundancy protocol (STP, RSTP, HIPER-Ring, ring coupling, dual homing) which is activated at this port.
- ▶ VLAN information concerning the port (VLAN ID and VLAN name).

This information can be called up from a network management station. With this information, the network management station is able to display the topology of the network.

LLDP uses an IEEE-MAC address for exchanging information. This address is normally not routed by switches. This is why switches without LLDP support drop the LLDP packets. Consequently, a non-LLDP-capable device between two LLDP-capable devices prevents the exchange of LLDP information. To avoid this, Hirschmann Switch send additional LLDP packets to the Hirschmann Multicast-MAC address 01:80:63:2F:FF:0B. Hirschmann Switch with the LLDP function are thus also able to exchange LLDP information with each other via devices which themselves are not LLDP-capable.

The Management Information Base (MIB) of an LLDP capable Hirschmann Switch holds out the LLDP information in the lldp-MIB and in the private hmlldp-MIB.



## 9.7.2 Displaying the topology discovery

- ☐ Select the `Diagnostics:Topology Discovery` dialog.

This dialogue offers you the possibility to switch on/off the function for topology discovery (LLDP).

The topology table shows you the selected information to neighbour devices.

The option “View LLDP entries exclusively” allows you to reduce the number of topology table entries. In this case the topology table hides entries of de-vices without active topology discovery function.

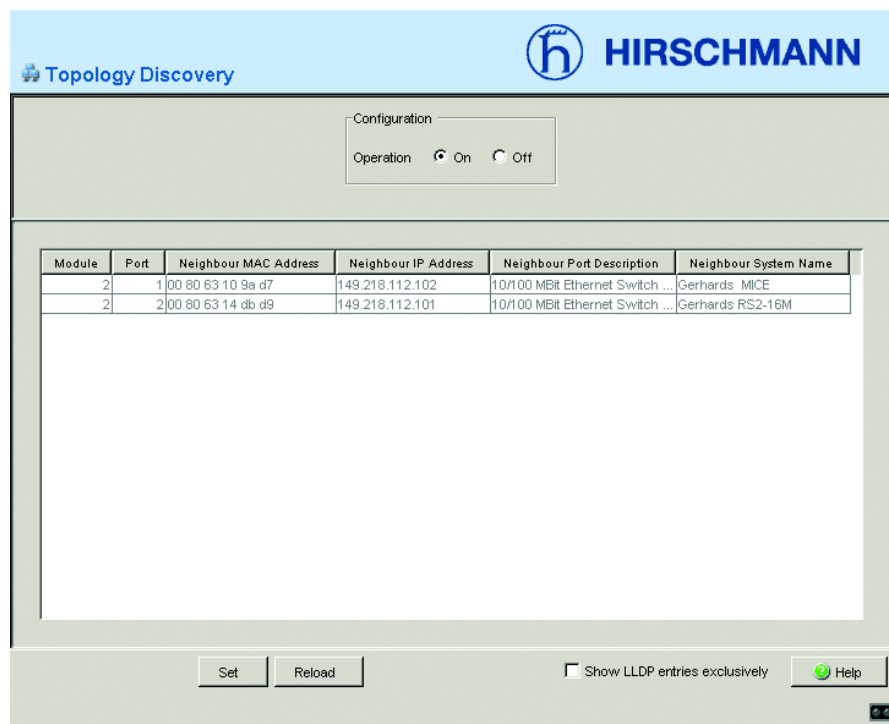


Fig. 54: Topology discovery dialog

If several devices are connected to a port, for example via a hub, the table shows one line for each connected device.

If

- ▶ devices with active topology discovery function and
  - ▶ devices without active topology discovery function
- are connected to a port, the topology table hides the devices without active topology discovery.

If

- ▶ only devices without active topology discovery
- are connected to a port, the table will contain one line for this port symbolically for all devices. The line contains the number of connected devices.

MAC addresses of devices that the topology table hides for the sake of clarity, are located in the Address Table (FDB, see [“Entering static address entries” on page 108](#)).

## 9.8 IP Address Conflict Detection

### 9.8.1 Description of IP address conflicts

By definition, each IP address may only be assigned once within a subnetwork. Should two or more devices erroneously share the same IP address within one subnetwork, this will inevitably lead to malfunctions including communication disruptions with devices that have this IP address.

In his Internet draft, Stuart Cheshire describes a mechanism that industrial Ethernet devices can use to detect and eliminate address conflicts (Address Conflict Detection, ACD).

Mode	Meaning
enable	Enables active and passive detection.
disable	Disables the function
activeDetectionOnly	Enables active detection only. After connection has been made to a network or after an IP address has been configured, the switch checks immediately if the IP address already exists within the network. If the IP address already exists, the switch will return to the previous configuration, if possible, and make another attempt after 15 seconds. At any rate, the switch will not connect to the network with a double IP address.
passiveOnly	Enables passive detection only. The switch listens passively to the network to determine if the IP address already exists. If it detects a double IP address, it will initially defend its address by employing the ACD mechanism and sending out gratuitous ARPs. If the remote connection does not disconnect from the network, the management interface of the local switch will then disconnect from the network. Every 15 seconds, it will poll the network to determine if there is still an address conflict. If not, it will connect back to the network.

*Table 13: Possible address conflict operation modes*

## 9.8.2 Configuring ACD

- ☐ Select the dialog `Diagnostics:IP Address Conflict Detection`.
- ☐ With “Status” you can enable or disable IP address conflict detection or select the operating mode ([see Tab. 13 on page 163](#)).

## 9.8.3 Displaying ACD

- ☐ Select the dialog `Diagnostics:IP Address Conflict Detection`.
- ☐ This dialog logs the IP address conflicts which the Switch detects, if it detects a conflict with its IP address.  
For each conflict, the Switch:
  - logs the time,
  - the conflicting IP address,
  - the MAC address of the device with which the IP address conflicted.The Switch writes one line to the log for each IP address that represents the last conflict that occurred.
- ☐ You can delete this table by restarting the Switch.

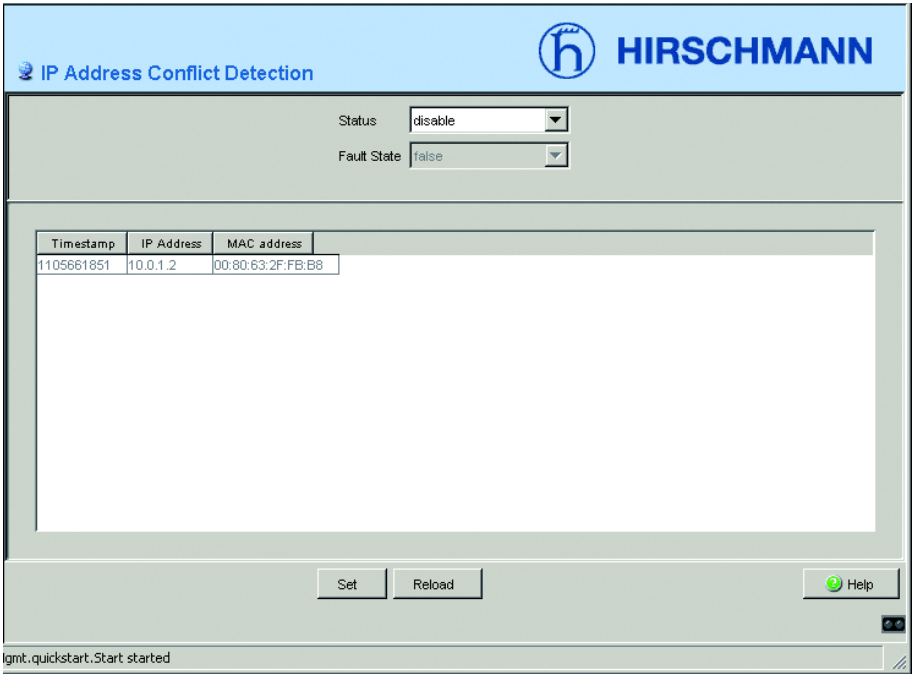



Fig. 55: IP address conflict detection

## 9.9 Reports

For diagnosis purposes, the Switch allows you to use the following reports:

- ▶ **Log File**  
The Log File is an HTML file in which the Switch records all important device internal events.
- ▶ **System Information**  
The system information is an HTML file containing all system relevant data.
- ▶ **System Information**  
The security data sheet IAONA is a data sheet in the XML format that has been standardized by IAONA (Industrial Automation Open Networking Alliance). Among other data, it contains security-related information on the accessible ports and the associated protocols.
- ▶ **Diagnostic table**  
The diagnostic table lists the alarms that were generated (traps).

These reports are available for diagnosis purposes. In service situations they report necessary information to the technician.

- 
- ☐ Select the `Diagnostics:Report` dialog.
  - ☐ Click “Log File” to open the HTML file in a new browser window.
  - ☐ Click “System information” to open the HTML file in a new browser window.

## 9.10 Monitoring port traffic (port mirroring)

In port mirroring, the data traffic related to a port, the source port, is copied to another port, the destination port. Data traffic at the source port is not influenced by port mirroring.

A management tool connected to the destination port, such as an RMON probe, can thus observe the data traffic at the source port.

The destination port forwards data to be sent and blocks received data.

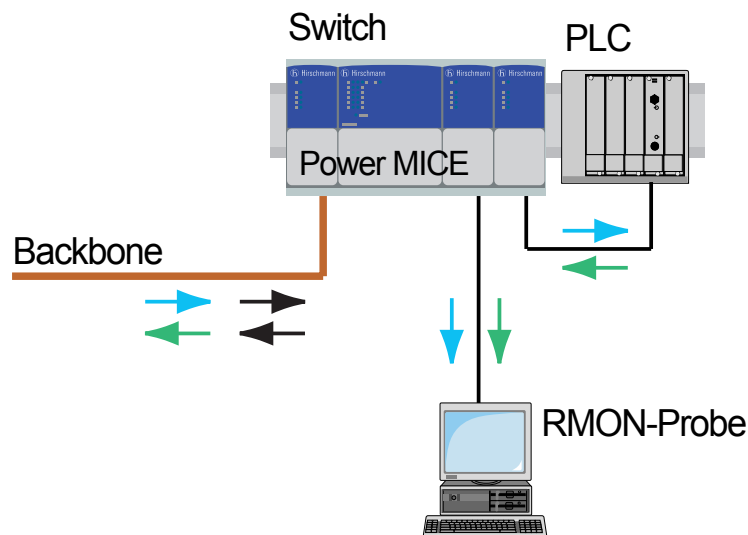


Fig. 56: Port Mirroring

- ☐ Select the `Diagnostics:Port Mirroring` dialog.

This dialog allows you to configure and activate the port mirroring function of the Switch.

- ☐ Select the source port whose data traffic you wish to monitor..
- ☐ Select the destination port to which you have connected your management tool.

- ☐ Select „enabled“, to enable the function.

The “Delete” button in the dialog allows you to restore all the default port mirroring settings (state on delivery).

**Note:** In active port mirroring, the specified port is used solely for observation purposes.

The screenshot shows a software dialog box titled "Port Mirroring" with the Hirschmann logo in the top right corner. The main area contains a table with two columns: "Module" and "Port". Below the table, there are two rows of input fields: "Source port" and "Destination port", each with a dropdown menu showing "1" and "0". Below these fields is a checkbox labeled "enabled". At the bottom of the dialog, there are four buttons: "Set", "Reload", "Delete", and "Help".

	Module	Port
Source port	1	0
Destination port	1	0

☐ enabled

Set Reload Delete Help

Fig. 57: Port mirroring dialog



# **Appendix A: Setting up the configuration environment**

## A.1 Setting up DHCP/BOOTP Server

On the CDROM supplied with the switch you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

- ☐ To install the DHCP server on your PC  
insert the CD-ROM into the CD drive of your PC and  
under Additional Software, select “haneWIN DHCP-Server”.  
To carry out the installation, follow the installation assistant.
- ☐ Start the DHCP Server program.

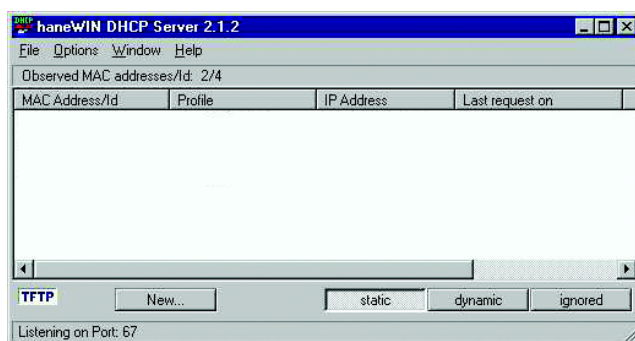


Fig. 58: Start window of the DHCP server

**Note:** The installation procedure includes a service which is automatically started in the basic configuration when switching on Windows. This service is even active if the program itself has not yet been started. The service started answers DHCP queries.

- ☐ Open the window for the program settings in the menu bar:  
Options: Preferences and select the DHCP tab page. Enter the settings shown in the illustration and click on OK.

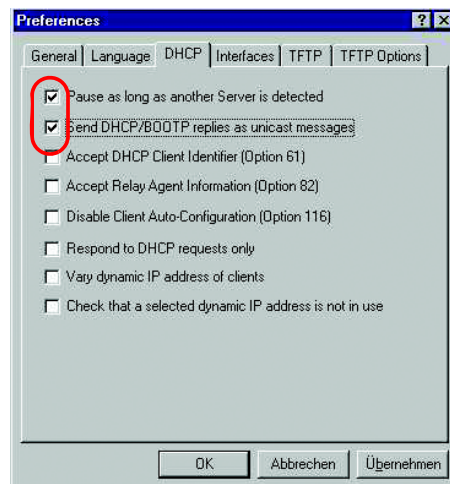


Fig. 59: DHCP setting

- ☐ To enter the configuration profiles, select manage in the menu bar of Options: Manage Profiles.
- ☐ Enter the name of the new configuration profile and click on New.

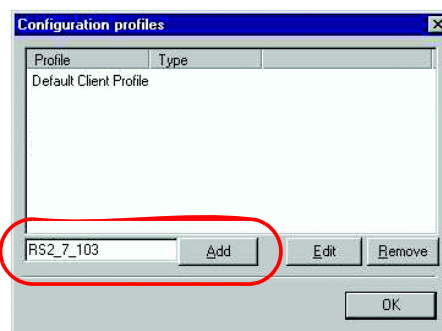


Fig. 60: Adding configuration profiles

- ☐ Enter the network mask and click on **Accept**.

The screenshot shows the 'Basic Profile' tab of the 'RS2\_7\_103' configuration window. The 'for:' dropdown is set to 'static Entries'. Under 'Dynamic IP Addresses', the 'Subnet mask' field is highlighted with a red circle and contains the value '255.255.255.0'. Other fields include 'Lease time (s): 36000', 'Gateway Address:', 'Backup Gateway 1:', and 'Backup Gateway 2:'. At the bottom, the 'Übernehmen' button is highlighted with a red circle.

**Fig. 61:** Network mask in the configuration profile

- ☐ Select the **Boot** tab page.
- ☐ Enter the IP address of your tftp server.
- ☐ Enter the path and the file name for the configuration file.
- ☐ Click on **Apply** and then on **OK**.

The screenshot shows the 'Boot' tab of the 'RS2\_7\_103' configuration window. The 'Name' field is highlighted with a red circle and contains the value '149.218.112.159'. The 'File' field contains the value '/switch/103config.dat'. Other fields include 'Next Server IP Address:', 'Boot File Size (in 512 byte blocks):', 'Always use option 66/67 for Name and File:', 'Alternate File if Vendor-Class-Id is:', and 'Root Path:'. At the bottom, the 'Übernehmen' button is highlighted with a red circle.

**Fig. 62:** Configuration file on the tftp server

- ☐ Add a profile for each device type.  
If devices of the same type have different configurations, then you add a profile for each configuration.  
To complete the addition of the configuration profiles, click on **OK**.

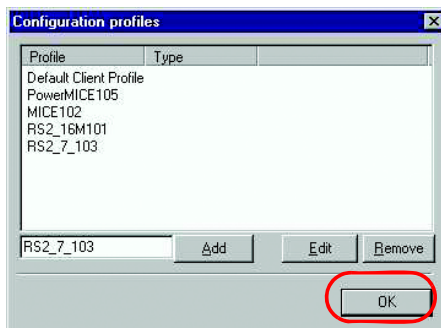


Fig. 63: Managing configuration profiles

- ☐ To enter the static addresses, click on **Static** in the main window.

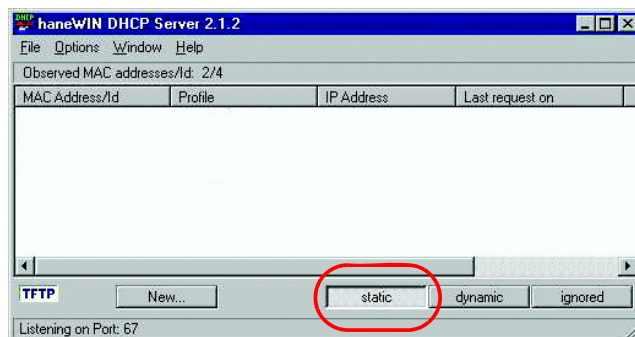
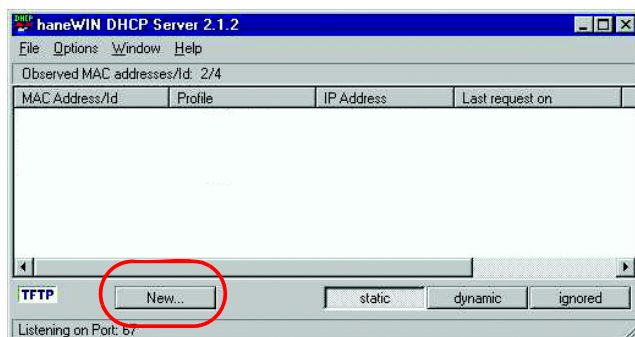


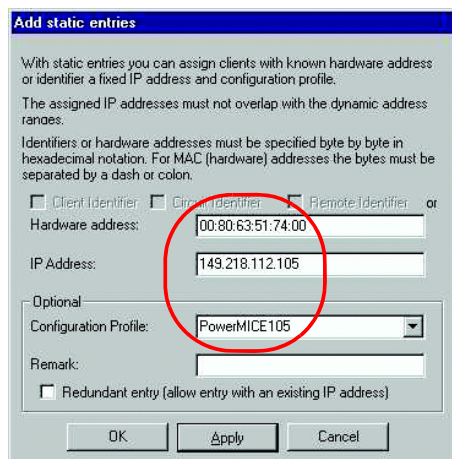
Fig. 64: Static address input

- ☐ Click on New.



**Fig. 65:** Adding static addresses

- ☐ Enter the MAC address of the switch.
- ☐ Enter the IP address of the switch.
- ☐ Select the configuration profile of the switch.
- ☐ Click on Accept and then on OK.



**Fig. 66:** Entries for static addresses

- ☐ Add an entry for each device that will get its parameters from the DHCP server.

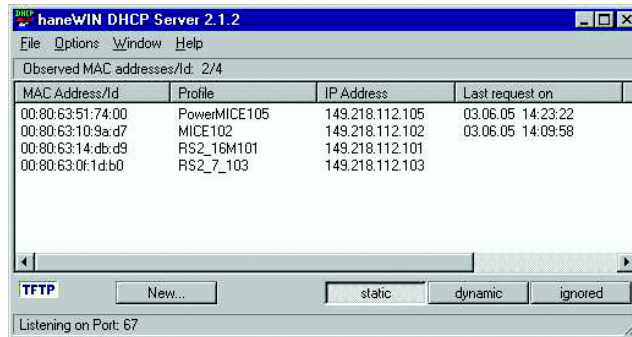
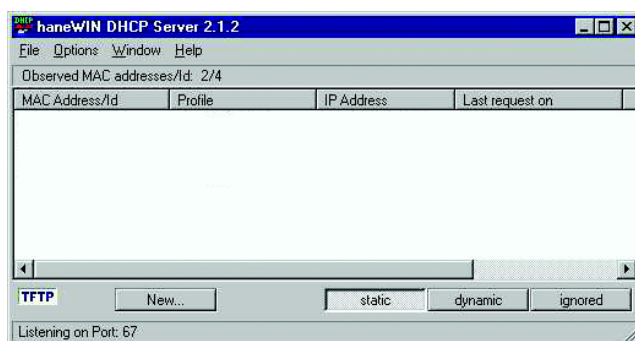


Fig. 67: DHCP server with entries

## A.2 Setting up DHCP Server Option 82

On the CDROM supplied with the switch you will find the software for a DHCP server from the software development company IT-Consulting Dr. Herbert Hanewinkel. You can test the software for 30 calendar days from the date of the first installation, and then decide whether you want to purchase a license.

- ☐ To install the DHCP server on your PC  
insert the CD-ROM into the CD drive of your PC and  
under Additional Software, select “haneWIN DHCP-Server”.  
To carry out the installation, follow the installation assistant.
- ☐ Start the DHCP Server program.



*Fig. 68: Start window of the DHCP server*

**Note:** The installation procedure includes a service which is automatically started in the basic configuration when switching on Windows. This service is even active if the program itself has not yet been started. The service started answers DHCP queries.



- ☐ Select `static`.

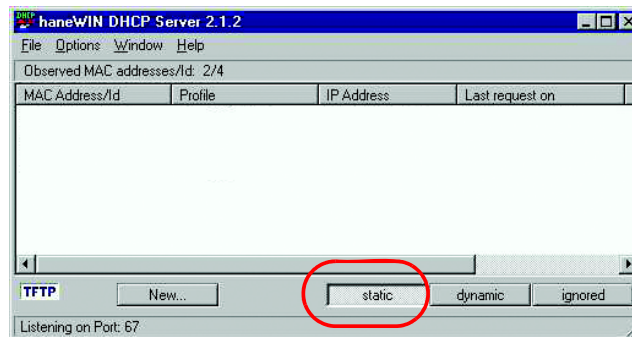


Fig. 69: Static address input

- ☐ Open the window for the program settings in the menu bar: `Options: Preferences` and select the `DHCP` tab page.
- ☐ Select the `DHCP` tab page. Enter the settings shown in the illustration and click on `OK`.

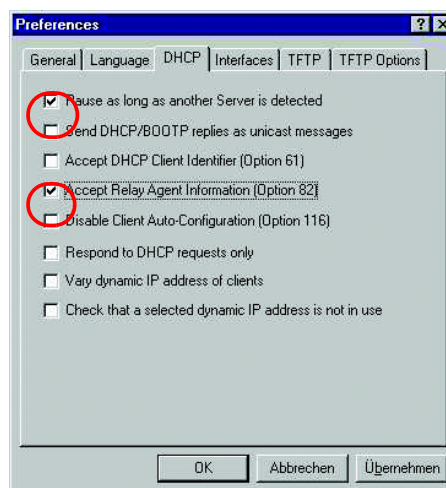


Fig. 70: DHCP setting

☐ To enter the static addresses, click on Add.

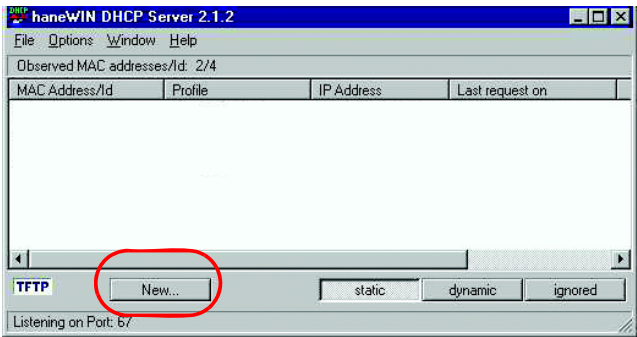


Fig. 71: Adding static addresses

☐ Select Circuit Identifier and Remote Identifier.

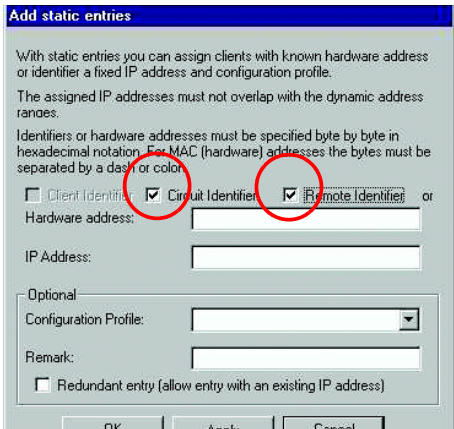


Fig. 72: Default setting for the fixed address assignment

- ☐ In the `Hardware address` field, you enter the `Circuit Identifier` and the `Remote Identifier`, see “Configuring the DHCP Relay Agent” in the reference guide “Web-based Interface”.

With `Hardware address` you identify the switch and the port to which that device is connected, to which you want to assign the IP address in the line below it.

The hardware address is in the following form:

```
ciclhhvvvssmmpprirlxxxxxxxxxxxx
```

- ▶ `ci`: sub-identifier for the type of the circuit ID
- ▶ `cl`: length of the circuit ID
- ▶ `hh`: Hirschmann identifier: `01` if a Hirschmann switch is connected to the port, otherwise `00`.
- ▶ `vvvv`: VLAN ID of the DHCP request (default: `0001` = VLAN 1)
- ▶ `ss`: socket of switch at which the module with that port is located to which the device is connected. Enter the value `00`.
- ▶ `mm`: module with the port to which the device is connected. Enter the value `00`.
- ▶ `pp`: port to which the device is connected.
- ▶ `ri`: sub-identifier for the type of the remote ID
- ▶ `rl`: length of the remote ID
- ▶ `xxxxxxxxxxxx`: remote ID of the switch (e.g. MAC address) to which a device is connected.

Fig. 73: Entering the addresses

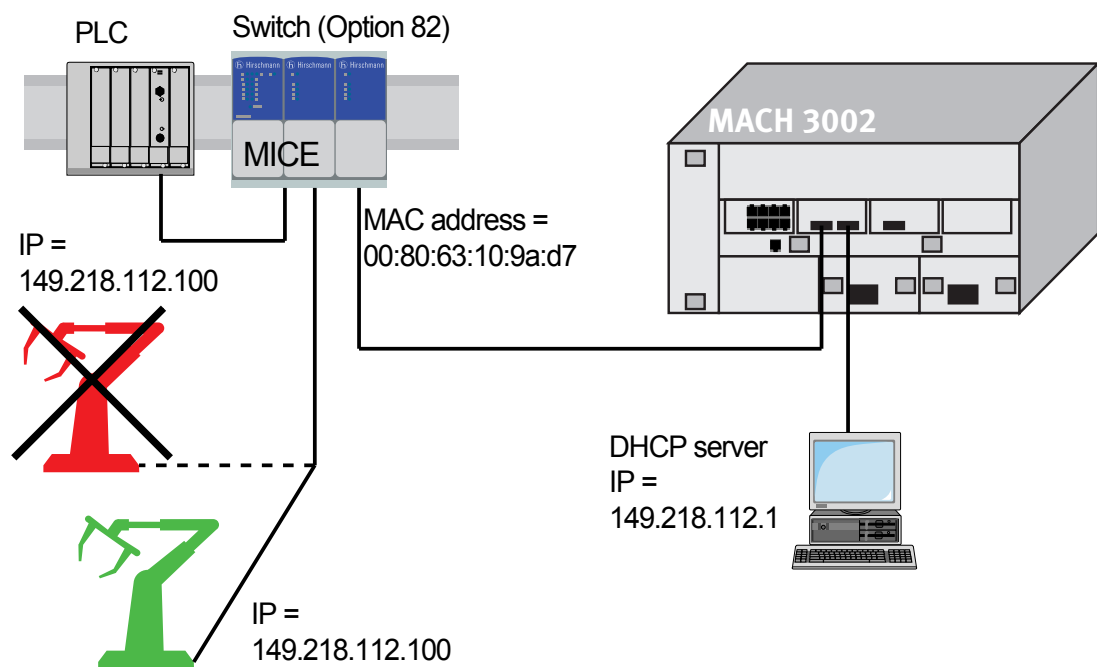


Fig. 74: Application example of using Option 82

## A.3 tftp server for software updates

On delivery, the switch software is held in the flash memory. The Switch boots the software from the flash memory.

Software updates can be realized via a tftp server. This presupposes that a tftp server has been installed in the connected network and that it is active.

**Note:** An alternative to the tftp update is the http update. The http update saves you having to configure the tftp server.

The Switch requires the following information to be able to make a software update from the tftp server:

- ▶ its own IP address (entered permanently),
- ▶ the IP address of the tftp server or gateway to the tftp server,
- ▶ the path in which the operating system of the tftp server is kept

File transfer between Switch and tftp server is handled by way of the **T**rivial **F**ile **T**ransfer **P**rotocol (tftp).

Management station and tftp server may be made up of one or more computers.

Preparation of the tftp server for the Switch software involves the following steps:

- ▶ Setting-up the Switch directories and copying the Switch software
- ▶ Setting-up the tftp process

## A.3.1 Setting up the tftp process

General prerequisites:

- ▶ The local address of the Switch and the IP address of the tftp servers or the gateway are known to the Switch.
- ▶ The TCP/IP stack with tftp is installed on tftp server.

The following sections contain information on setting up the tftp process, arranged according to operating system and application.

### ■ SunOS and HP

- ☐ First check whether the tftp daemon (background process) is running, i.e. whether the file `/etc/inetd.conf` contains the following line (see Fig. 75) and whether the status of this process is “IW”:

SunOS

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd
-s /tftpboot
```

HP

```
tftp dgram udp wait root /usr/etc/in.tftpd tftpd
```

If the process is not in the file, or if the related line is commented out (#), modify `/etc/inetd.conf` accordingly and then re-initialize the INET daemon. This is done with the command “kill -1 PID”, where PID is the process ID of `inetd`.

This re-initialization can be executed automatically by inputting the following UNIX commands:

SunOS

```
ps -ax | grep inetd | head -1 | awk -e {print $1} |
kill -1
```

HP

```
/etc/inetd -c
```

You can obtain additional information about the tftpd daemon tftpd with the UNIX command “man tftpd”.

**Hinweis:** The command “ps” does not always show the tftp daemon, although it is actually running.

Special steps for HP workstations:

- ☐ During installation on an HP workstation, enter the user tftp in the /etc/passwd file.

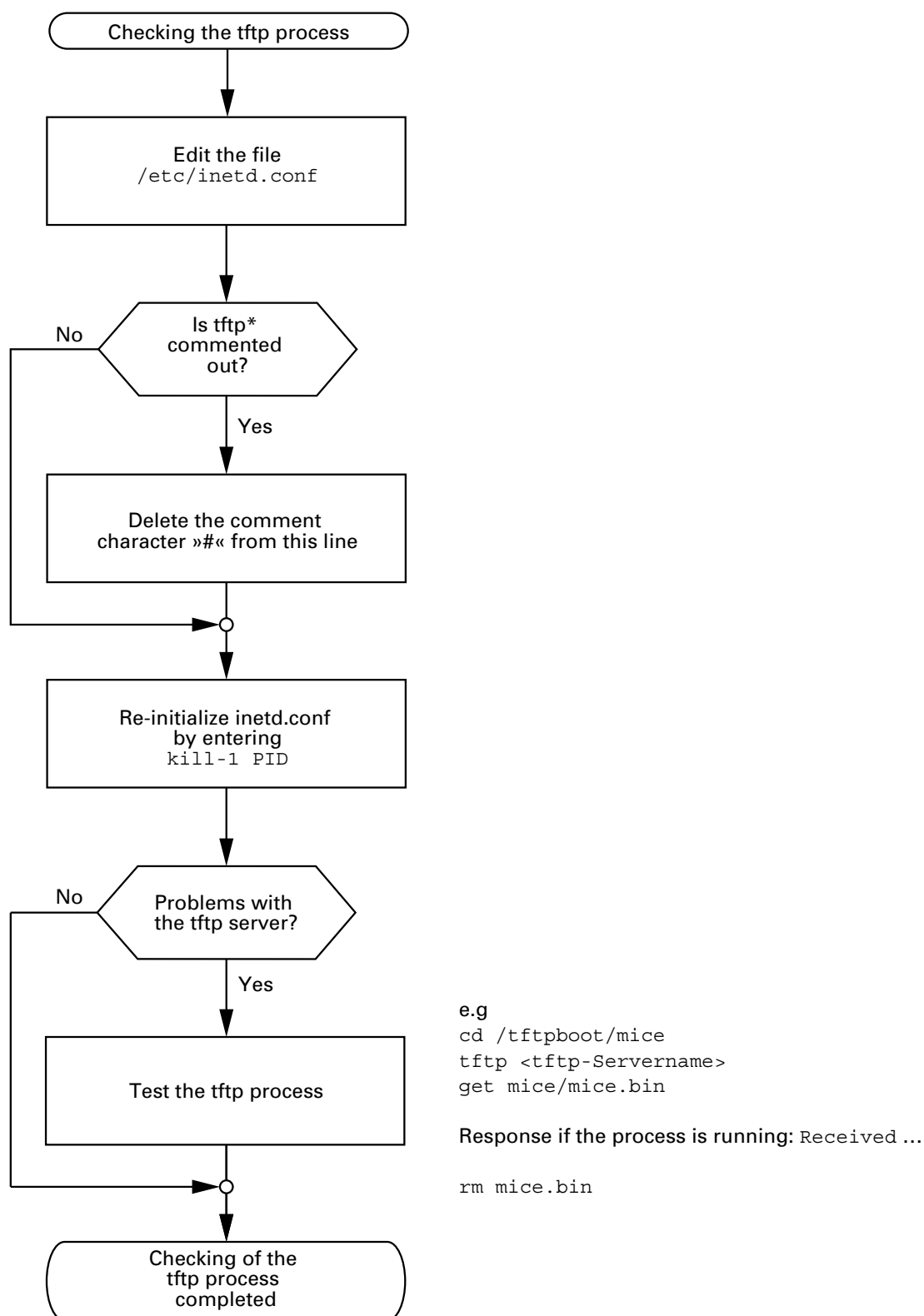
For example:

```
tftp:*:510:20:tftp server:/usr/tftpd:/bin/false
```

tftp	user ID,
*	is in the password field,
510	sample user ID,
20	sample group ID,
tftp server	freely selectable designation,
/bin/false	mandatory entry (login shell)

- ☐ Test the tftp process with, for example:

```
cd /tftpboot/mice
tftp <tftp-Servername>
get mice/mice.bin
rm mice.bin
```



\* tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot

Fig. 75: Flow chart for setting up tftp server with SunOS and HP



## A.3.2 Software access rights

The agent needs read permission to the tftp directory with the Switch software.

### ■ Example of a UNIX tftp server

Once Switch software has been installed, the tftp server should have the following directory structure with the stated access rights:

Filename	Access
mice.bin	444-r--r--r--

*Table 14: Directory structure of the software*

d = directory; r = read; w = write; x = execute

1st position designates d (directory),

2nd to 4th positions designate user access rights,

5th to 7th positions designate access rights of user groups,

8th to 10th positions designate access rights of all others.



# **Appendix B: General Information**

## B.1 Hirschmann Competence

In the longterm, product excellence alone is not an absolute guarantee of a successful project implementation. Comprehensive service makes a difference worldwide. In the current scenario of global competition, the Hirschmann Competence Center stands head and shoulders above the competition with its comprehensive spectrum of innovative services:

- ▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- ▶ Training offers you an introduction to the technological fundamentals, product briefing and user training with certification.
- ▶ Support ranges from commissioning through the standby service to maintenance concepts.

With the Competence Center, you firmly rule out any compromise: the client-specific package leaves you free to choose the service components that you will use.

Internet:

<http://www.hicomcenter.com>

## B.2 FAQ

Answers to frequently asked questions can be found at the Hirschmann Website:

[www.hirschmann.com](http://www.hirschmann.com)

Under Products/Support inside Automation and Network Solutions is located on the pages Products the area FAQ.

For detailed information on all services offered by the Hirschmann Competence Center, please visit the Web site <http://www.hicomcenter.com/>.

## B.3 Management Information BASE MIB

The Management Information Base (MIB) is designed in the form of an abstract tree structure.

The branching points are the **object classes**. The “leaves” of the MIB are called **generic object classes**.

Wherever necessary for unambiguous identification, the generic object classes are **instantiated**, i.e. the abstract structure is imaged on the reality, by specifying the port or the source address.

Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified.

The **object description** or the **object ID** (OID) identifies the object class.

The **subidentifier** (SID) is used for instantiation.

### Example:

The generic object class

```
hmPSState (OID = 1.3.6.1.4.1.248.14.1.2.1.3)
```

is the description of the abstract information “power supply state”. However, it is not possible to read any information from this, as the system does not know which power supply is meant.

Specification of the subidentifier (2) images this abstract information onto reality (instantiates it), which means that it refers to power supply 2. A value is assigned to this instance and can then be read. The instance “get 1.3.6.1.4.1.248.14.1.2.1.3.2”, for example, returns the response “1”, which means that the power supply unit is ready for operation.

The following abbreviations are used in the MIB:

Comm	Group access rights
con	Configuration
Descr	Description
Fan	Fan
ID	Identifier
Lwr	Lower (e.g. threshold value)
PS	Power supply
Pwr	Power

sys	System
UI	User Interface
Upr	Upper (e.g. threshold value)
ven	Vendor = manufacturer (Hirschmann)

**Definition of the syntax terms used:**

Integer	An integer in the range 0 - 2 <sup>32</sup>
IP address	xxx.xxx.xxx.xxx (xxx = integer in the range 0-255)
MAC address	12-digit hexadecimal number in accordance with ISO / IEC 8802-3
Object Identifier	x.x.x.x... (e.g. 1.3.6.1.1.4.1.248...)
Octet String	ASCII character string
PSID	Power Supply Identification (number of the power supply unit)
TimeTicks	Stopwatch Elapsed time (in seconds) = numerical value / 100 Numerical value = integer in the range 0 - 2 <sup>32</sup>
Timeout	Time value in hundredths of a second Time value = integer in the range 0-2 <sup>32</sup>
Type field	4-digit hexadecimal number in accordance with ISO / IEC 8802-3
Counter	Integer (0 - 2 <sup>32</sup> ) whose value is incremented by 1 when certain events occur.

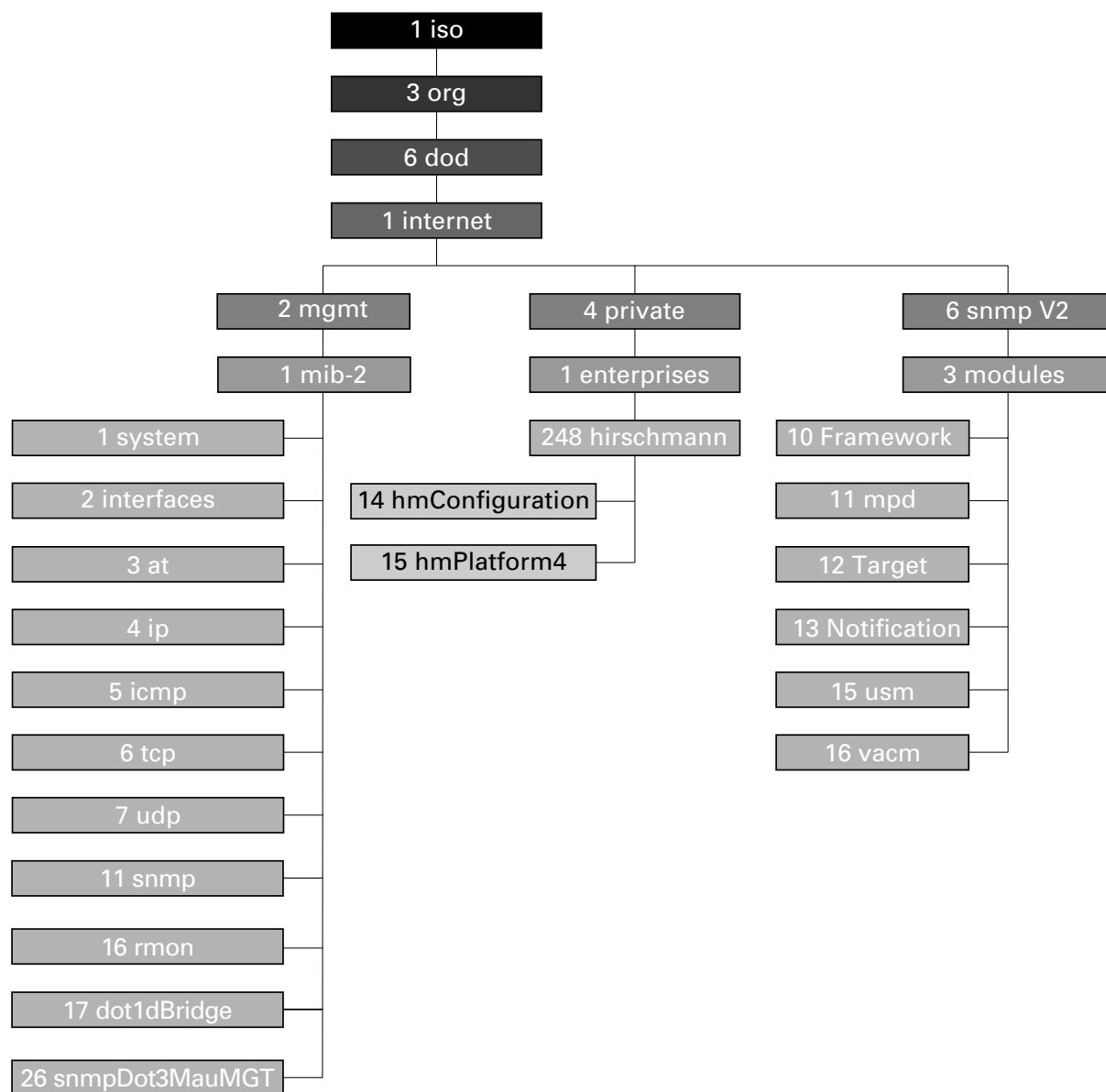


Fig. 76: Tree structure of the Hirschmann MIB

A complete description of the MIB can be found on the CD-ROM that is included with the device.



## B.4 Used abbreviations

ACA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol)
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
http	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocoll
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocoll
LWL	Lichtwellenleiter
MAC	Media Access Control
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundanz Manager
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transfer Control Protocol
tftp	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagramm Protocol
URL	Uniform Resourve Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

## B.5 List of RFC's

- ▶ RFC 768 (UDP)
- ▶ RFC 783 (TFTP)
- ▶ RFC 791 (IP)
- ▶ RFC 792 (ICMP)
- ▶ RFC 793 (TCP)
- ▶ RFC 826 (ARP)
- ▶ RFC 854 (Telnet)
- ▶ RFC 855 (Telnet Option)
- ▶ RFC 951 (BOOTP)
- ▶ RFC 1112 (IGMPv1)
- ▶ RFC 1157 (SNMPv1)
- ▶ RFC 1155 (SMIv1)
- ▶ RFC 1212 (Concise MIB Definitions)
- ▶ RFC 1213 (MIB2)
- ▶ RFC 1493 (Dot1d)
- ▶ RFC 1542 (BOOTP-Extensions)
- ▶ RFC 1643 (Ethernet-like -MIB)
- ▶ RFC 1757 (RMON)
- ▶ RFC 1769 (SNTP)
- ▶ RFC 1867 (HTML/2.0 Forms w/ file upload extensions)
- ▶ RFC 1901 (Community based SNMP v2)
- ▶ RFC 1905 (Protocol Operations for SNMP v2)
- ▶ RFC 1906 (Transport Mappings for SNMP v2)
- ▶ RFC 1907 (Management Information Base for SNMP v2)
- ▶ RFC 1908 (Coexistence between SNMP v1 and SNMP v2)
- ▶ RFC 1945 (HTTP/1.0)
- ▶ RFC 2068 (HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03)
- ▶ RFC 2131 (DHCP)
- ▶ RFC 2132 (DHCP-Options)
- ▶ RFC 2233 - The Interfaces Group MIB using SMI v2
- ▶ RFC 2236 (IGMPv2)
- ▶ RFC 2246 (The TLS Protocol, Version 1.0)
- ▶ RFC 2271 (SNMP Framework MIB)
- ▶ RFC 2346 (AES Ciphersuites for Transport Layer Security)
- ▶ RFC 2570 (Introduction to SNMP v3)
- ▶ RFC 2571 (Architecture for Describing SNMP Management Frameworks)
- ▶ RFC 2572 (Message Processing and Dispatching for SNMP)
- ▶ RFC 2573 (SNMP v3 Applications)

- ▶ RFC 2574 (User Based Security Model for SNMP v3)
- ▶ RFC 2575 (View Based Access Control Model for SNMP)
- ▶ RFC 2576 (Coexistence between SNMP v1,v2 & v3)
- ▶ RFC 2578 (SMI v2)
- ▶ RFC 2579 (Textual Conventions for SMI v2)
- ▶ RFC 2580 (Conformance statements for SMI v2)
- ▶ RFC 2613 (SMON)
- ▶ RFC 2618 (RADIUS Authentication Client MIB)
- ▶ RFC 2620 (RADIUS Accounting MIB)
- ▶ RFC 2674 (Dot1p/Q)
- ▶ RFC 2818 (HTTP over TLS)
- ▶ RFC 2851 (Internet Addresses MIB)
- ▶ RFC 2865 (RADIUS Client)
- ▶ RFC 2866 (RADIUS Accounting)
- ▶ RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)
- ▶ RFC 2869 (RADIUS Extensions)
- ▶ RFC 2869bis (RADIUS support for EAP)
- ▶ RFC 2933 (IGMP MIB)
- ▶ RFC 3376 (IGMPv3)
- ▶ RFC 3580 (802.1X RADIUS Usage Guidelines)

## B.6 Based IEEE standards

- ▶ IEEE 802.1AB Topologie Discovery (LLDP)
- ▶ IEEE 802.1 D Switching, GARP, GMRP, Spanning Tree  
(Supported via 802.1S implementation)
- ▶ IEEE 802.1 D-1998 Media access control (MAC) bridges  
(includes IEEE 802.1p Priority and Dynamic Multi-cast Filtering, GARP, GMRP)
- ▶ IEEE 802.1 Q-1998 Virtual Bridged Local Area Networks  
(VLAN Tagging, Port Based VLANs, GVRP)
- ▶ IEEE 802.1 w.2001 Rapid Reconfiguration (RSTP)
- ▶ IEEE 802.1 X Port Authentication
- ▶ IEEE 802.3 - 2002 Ethernet
- ▶ IEEE 802.3 ac VLAN Tagging
- ▶ IEEE 802.3 ad Link Aggregation with Static LAG and LACP support  
(Power MICE and MACH 4000)
- ▶ IEEE 802.3 x Flow Control
- ▶ IEEE 802.1 af Power over Ethernet

# B.7 Technical Data

<b>■ VLAN</b>	
VLAN ID	1 to 4042 (MACH 4000: 3966)
Number of VLANs	max. 256 simultaneously per switch max. 256 simultaneously per port
Number of VLANs with GMRP	
in VLAN 1	max. 256 simultaneously per switch
in VLAN 1	max. 256 simultaneously per port

## **B.8 Copyright of integrated software**

### **B.8.1 Bouncy Castle Crypto APIs (Java)**

The Legion Of The Bouncy Castle  
Copyright (c) 2000 The Legion Of The Bouncy Castle  
(<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### **B.8.2 LVL7 Systems, Inc.**

(c) Copyright 1999-2006 LVL7 Systems, Inc. All Rights Reserved.

# B.9 Reader's comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your **assessment** of this manual:

	excellent	good	satisfactory	mediocre	poor
Accuracy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Readability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Comprehensibility	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Examples	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Structure/Layout	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Completeness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Graphics	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Drawings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tables	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Did you discover an error in the manual?  
If so, on what page?

.....

.....

.....

.....

.....

.....

.....

**Suggestions for improvement and additional information:**

.....

.....

.....

.....

**General comments:**

.....

.....

.....

.....

Company / Department .....

Name / Telephone number .....

Street .....

Zip code / City .....

Date / Signature .....

Dear User,

Please fill out and return this page

- by fax to the number +49 (0)7127/14-1798 or
- by mail to  
Hirschmann Automation and Control GmbH  
Department AMM  
Stuttgarter Str. 45 - 51

72654 Neckartenzlingen  
Germany



# Appendix C: Index

<b>A</b>			EtherNet/IP	9
ACA	37, 53, 63, 65, 146		Event counters	156
Access right	74			
ACD	163	<b>F</b>		
Address conflict	163	FAQ		189
Address Conflict Detection	163	Faulty Device Replacement		49
Address table	107	FDB		108
Aging Time	107, 112	Filter		108
Alarm	84, 144	Filter table		108
Alarm messages	142	First installation		25
Allowed IP addresses	84	Flow control		124
Allowed MAC addresses	84	Forwarding Database		108
APNIC	27			
ARIN	27	<b>G</b>		
Authentication	145	gateway		34
AutoConfiguration Adapter	146	Generic object classes		190
		GMRP		109, 110
		Grandmaster		95
<b>B</b>				
Bandwidth	110, 124	<b>H</b>		
Booting	16	HaneWin		170, 176
BOOTP	25, 44, 47	Hardware address		40
Boundary	99	Hardware reset		142
Boundary clock	97	HiDiscovery		48, 81
Broadcast	93, 106, 110, 127	HIPER-Ring		146
Broadcast address	108	HiVision		44
Browser	22			
		<b>I</b>		
<b>C</b>		IANA		27
CD-ROM	170, 176	IAONA		166
Chassis	146	IEEE 802.1 Q		119
CLI	75	IEEE-MAC address		160
Clock	95	IGMP		109
Closed circuit	150	IGMP Snooping		110
Cold Start	145	Industry Protocols		9
Configuration data	39, 46, 54, 57	Ingress Filter		131, 138
Configuration modifications	142	Ingress rule		127
Coupling	146	Instantiation		190
		Internet Assigned Numbers Authority		27
<b>D</b>		Internet Service Provider		27
Destination address	108, 109	IP address		25, 27, 33, 40, 43, 48, 81, 84, 163, 181
Destination address field	106	ISO/OSI layer model		31
Destination port	167			
Device state	147	<b>J</b>		
DHCP	25, 33	JavaScript		23
DHCP client	43			
DHCP Option 82	46	<b>L</b>		
DHCP server	170, 176	LACNIC		27
		Leave		112
<b>E</b>				
Egress rule	127			

Link Down	145	<b>Q</b>	
Link up	145	QoS	119
LLDP	161	Queue	121
Local clock	96		
Logical communication path	97	<b>R</b>	
Login	23	Real time	87, 119
		Receiving port	109
<b>M</b>		Redundancy	146
MAC	96	Redundancy manager	108
MAC address	43, 48, 81, 84	Reference clock	95
MAC destination address	31	Relay contact	150
Media module	146	Release	61
Member	131	Report	112
Member set	128	Restart	109, 156
Message	142	RFC	194
Multicast	93, 110, 112, 127	RIPE NCC	27
Multicast address	108	RMON probe	167
<b>N</b>		<b>S</b>	
Network address	27	Security Data Sheet IAONA	166
Network management	44	Segmentation	142
Network mask	33	Service provider	27
Network topology	46	Signaling Relay	146
NTP	90	Simple PTP Mode	99
		SNMP	22, 74, 75, 77, 142
<b>O</b>		SNMPv1/2c	77
Object classes	190	SNTP cascade	90
Object description	190	SNTP Client	90
Object ID	190	SNTP Server	90
Option 82	26, 46, 176	Software	185
Ordinary clock	97	Source address	106
Overload protection	124	Source port	167
		State on delivery	74
<b>P</b>		Static	108
Password	20, 74, 75	Strict priority	121
PHY layer	96	Subdomain	97
Polling	142	Subidentifier	190
Port Configuration	69	Subnetwork	33, 107
Port Mirroring	167	Support	189
Port Security	85, 146	Synchronizing clocks	96
Port VLAN ID	127	System monitor	16
Power Supply	146	System name	43
Precision Time Protocol	95	System time	93
Preferred Master	99		
Priority	119, 120	<b>T</b>	
Priority queues	119	TCP/IP stack	182
Priority tagged frames	120	Telnet	19
PROFINET	9	Temperature threshold	146
Protocol stack	96	Time management	95
PTP	95	Time stamp unit	96
PTP Preferred Master	99	Topology	46
PTP-Subdomain	97	Traffic classes	119
		Transmission security	142
		Trap	84, 142, 144

Trap destination table	142
Trivial File Transfer Protocol	181
Type field	119

### U

Unicast	110
Universal Time Coordinated	90
Untagged set	128
User group	127
Username	20
UTC	90

### V

V.24	19
Video	121
VLAN	92, 119, 126
VLAN ID	47
VLAN identification	127
VLAN tag	119, 120, 127
VoIP	121

### W

Web-based interface	22
Web-based management	23







**HIRSCHMANN**

A Belden Company